# 3Com® Network Administrator
## for HP OpenView | Windows

# User Guide

3C15400

`http://www.3com.com/`

Part No. DUA1540-0AAA01
Published November 2003

**3Com Corporation**
**350 Campus Drive**
**Marlborough**
**MA USA 01752-3064**

3Com Technologies reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Technologies to provide notification of such revision or change.

3Com Technologies provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

**UNITED STATES GOVERNMENT LEGEND**

*If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:*

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com and the 3Com logo are registered trademarks of 3Com Corporation. XRN is a trademark of 3Com Corporation

IEEE and 802 are registered trademarks of the Institute of Electrical and Electronics Engineers, Inc.

Intel and Pentium are registered trademarks of Intel Corporation. Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Novell and NetWare are registered trademarks of Novell, Inc. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

Netscape Navigator is a registered trademark of Netscape Communications.

HP OpenView is a registered trademark of Hewlett Packard.

JavaScript is a trademark of Sun Microsystems.

All other company and product names may be trademarks of the respective companies with which they are associated.

**ENVIRONMENTAL STATEMENT**

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

**End of Life Statement**

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

**Regulated Materials Statement**

3Com products do not contain any hazardous or ozone-depleting material.

**Environmental Statement about the Documentation**

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally-friendly, and the inks are vegetable-based with a low heavy-metal content.

# CONTENTS

## ABOUT THIS GUIDE

## 1 GETTING STARTED

## 2 PRODUCT ACTIVATION

## 3 DEVICE WINDOW

## 4 Device Administration

## 5 Importing and Refreshing Devices

## 10 HP OPENVIEW INTEGRATION

## 11 LIVE UPDATE

## A SUPPORTED DEVICES

## B 3COM DEVICE VIEW

## C OBTAINING SUPPORT FOR YOUR PRODUCT

# ABOUT THIS GUIDE

This guide is intended for use by those responsible for installing, setting up and managing a network; consequently, it assumes a working knowledge of networks and network management systems.

*If the Release Notes provided with this 3Com® Network Administrator User Guide contain details that differ from the information in this guide, follow the information in the release notes.*

Most 3Com user guides are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the 3Com World Wide Web site:

**`http://www.3com.com/`**

## Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

**Table 1** Notice Icons

| Icon | Notice Type | Description |
|---|---|---|
| ℹ | Information note | Information that describes important features or instructions. |
| ⚠ | Caution | Information that alerts you to potential loss of data or potential damage to an application, system, or device. |
| ⚡ | Warning | Information that alerts you to potential personal injury. |

**Table 2** Text Conventions

| Convention | Description |
|---|---|
| `Screen displays` | This typeface represents information as it appears on the screen. |
| `Syntax` | The word "syntax" means that you must evaluate the syntax provided and then supply the appropriate values for the placeholders that appear in angle brackets. Example:<br>To change your password, use the following syntax:<br>`system password <password>`<br>In this example, you must supply a password for <password>. |
| **`Commands`** | The word "command" means that you must enter the command exactly as shown and then press Return or Enter. Commands appear in bold. Example:<br>To display port information, enter the following command:<br>**`bridge port detail`** |
| The words "enter" and "type" | When you see the word "enter" in this guide, you must type something, and then press Return or Enter. Do not press Return or Enter when an instruction simply says "type." |
| Keyboard key names | If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example:<br>Press Ctrl+Alt+Del |
| Words in *italics* | Italics are used to:<br>■ Emphasize a point.<br>■ Denote a new term at the place where it is defined in the text.<br>■ Identify menu names, menu commands, and software button names. Examples:<br>From the *Help* menu, select *Contents*.<br>Click *OK*. |

## Feedback about this User Guide

Your suggestions are very important to us. They will help make our documentation more useful to you. Please e-mail comments about this document to 3Com at:

**pddtechpubs_comments@3com.com**

Please include the following information when commenting:

- Document title
- Part number
- Page number (if appropriate)

Example:

3Com Network Administrator for HP OpenView User Guide

DUA1540-0AAA01

Page 21

*Do not use this email address for technical support questions. For information about contacting Technical Support, please refer to* Appendix B *on* page 251.

## Related Documentation

In addition to this guide, 3Com Network Administrator provides on-line help which can be accessed through the application.

# 1 GETTING STARTED

## Introduction

This chapter contains introductory information about 3Com® Network Administrator for HP OpenView, how to install and activate the application and a brief summary of all its major features.

### What is 3Com Network Administrator

3Com Network Administrator for HP OpenView is an application that lets you perform administration tasks on a number of your 3Com devices at once. By using 3Com Network Administrator you can:

- Directly import device information from HP OpenView or text files.
- Access the Telnet or Web Management consoles of your 3Com devices
- Launch device-specific 3Com configuration applications such as Device View
- Backup and Restore device configurations over the network and even deploy setup configurations to a number of 3Com devices at once.
- Perform upgrades of your 3Com devices using a single update wizard tool
- Generate reports of detailed information about your 3Com devices
- Configure your network to use the quality of service (QoS) capabilities of your 3Com devices

## On the CD

The CD contains the following resources:

- A readme file for 3Com Network Administrator
- The 3Com Network Administrator installation program
- This 3Com Network Administrator user guide in PDF format
- Adobe Acrobat Reader
- 3Com Switch Manager
- 3Com Router Manager

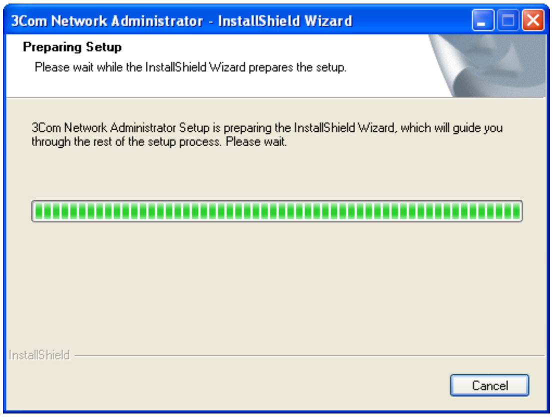
*Use Windows Explorer to browse the CD and access the files.*

## Installation

3Com recommends that you install the Router Manager and Switch Manager applications before you install 3Com Network Administrator. These applications must be installed first so that the 3Com Network Administrator installation can create the correct shortcuts to these applications.

To install 3Com Network Administrator, insert the product CD in your computer's CDROM drive and browse the CD. Double-click the `3Com Network Administrator v1.0.exe` file to begin the installation process. Once the installation has started (as shown in Figure 1), please follow the steps in the installation wizard.

**Figure 1** InstallShield Wizard



3Com Network Administrator - InstallShield Wizard

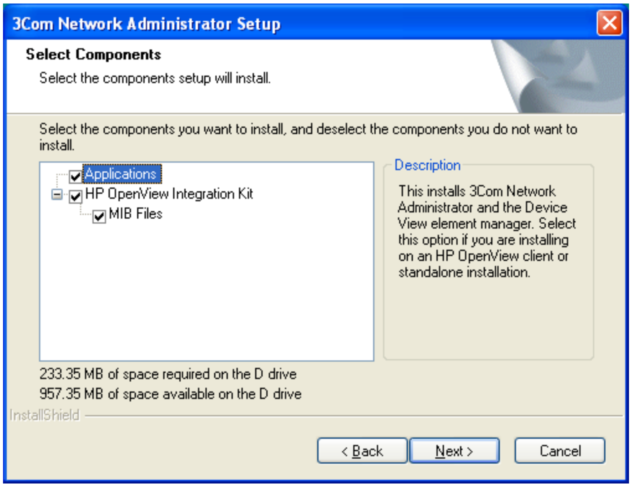
**Preparing Setup**

Please wait while the InstallShield Wizard prepares the setup.

3Com Network Administrator Setup is preparing the InstallShield Wizard, which will guide you through the rest of the setup process. Please wait.

The *Select Components* step in the installation wizard gives you the option of installing parts of 3Com Network Administrator as shown in Figure 2:

**Figure 2** Select Components



3Com Network Administrator Setup

**Select Components**

Select the components setup will install.

Select the components you want to install, and deselect the components you do not want to install.

- ☑ Applications
- ☑ HP OpenView Integration Kit
  - ☑ MIB Files

Description

This installs 3Com Network Administrator and the Device View element manager. Select this option if you are installing on an HP OpenView client or standalone installation.

233.35 MB of space required on the D drive
957.35 MB of space available on the D drive

The following table provides guidelines on the scenarios you may be installing 3Com Network Administrator under, and which checkboxes you should select:

**Table 3** Installation Checkboxes

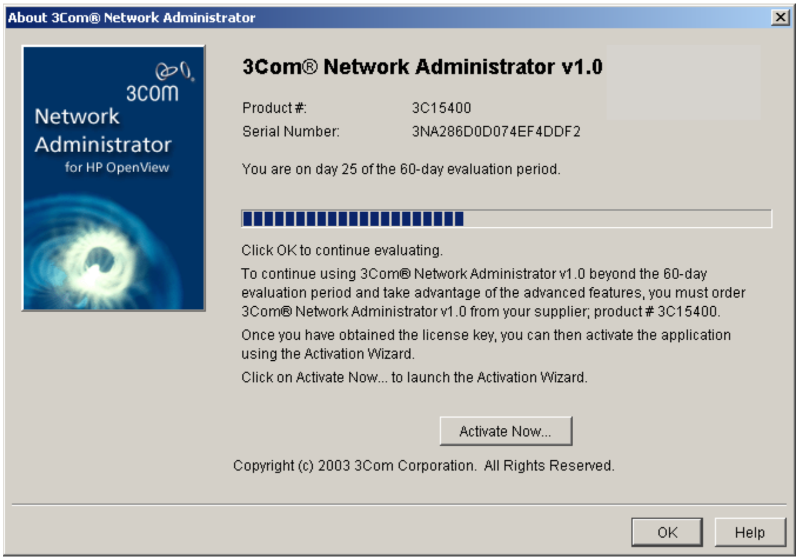
| | **Checkboxes:** | | |
|---|---|---|---|
| **Scenario** | **Applications** | **Integration** | **MIBs** |
| Installing 3Com Network Administrator on a system with a standalone version of HP OpenView | ✕ | ✕ | ✕ |
| Installing 3Com Network Administrator on a system that does not contain HP OpenView | ✕ | | |
| Installing 3Com Network Administrator on a system that is acting as an HP OpenView server.<br>Note: You must install on the server before installing any clients. | | ✕ | ✕ |
| Installing on a system that is an HP OpenView client. Please install the integration kit on the server before installing 3Com Network Administrator on any clients. | ✕ | | |

*Installing the MIBs into HP OpenView is optional. The MIBs give you access to low-level statistics and control of your 3Com devices. However, you may decide not to install the MIB collection to save time during the install, since the MIBs can take up to an hour to install.*

## Activation

Once you have installed 3Com Network Administrator, you will have a 60-day grace period within which to activate your software. When you launch 3Com Network Administrator for the first time the *About* dialog will be displayed as shown in Figure 3:

**Figure 3** About Dialog



3Com® Network Administrator v1.0

Product #: 3C15400
Serial Number: 3NA286D0D074EF4DDF2

You are on day 25 of the 60-day evaluation period.

Click OK to continue evaluating.

To continue using 3Com® Network Administrator v1.0 beyond the 60-day evaluation period and take advantage of the advanced features, you must order 3Com® Network Administrator v1.0 from your supplier; product # 3C15400.

Once you have obtained the license key, you can then activate the application using the Activation Wizard.

Click on Activate Now... to launch the Activation Wizard.

Copyright (c) 2003 3Com Corporation. All Rights Reserved.

To activate your software:

1. Click *Activate Now* to launch the Activation Wizard.
2. The wizard will ask you for your license key. Enter the key and click *Next*.

   3Com Network Administrator will then direct you to a 3Com activation website to retrieve your activation key.
3. Once you have your activation key, enter it into the *Activation Key* text box and click *Finish* to complete the activation process.

   For more information, please refer to "Product Activation" on page 27.

## Getting Started

This section details the two operations you need to perform before you can start using 3Com Network Administrator with your 3Com devices.

### Creating a New Inventory File

3Com Network Administrator stores detailed information about your 3Com devices in inventory files. When you first run 3Com Network Administrator, a *Welcome* dialog is displayed which lets you:

- Create a new inventory file
- Open an existing inventory file
- Open the last inventory file you were using

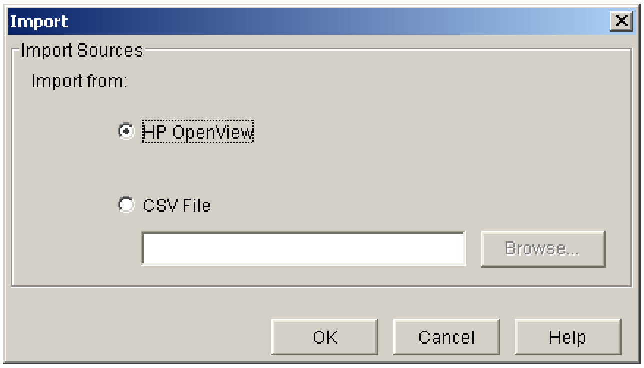
To create a new inventory file from the *Welcome* dialog, select *Create a new inventory file* and click *OK*.

### Import Device Information

Once you have an inventory file loaded into 3Com Network Administrator, you must bring device information into the import facility as follows:

**1** From the *File* menu, select *Import* to display the dialog shown in Figure 4:

**Figure 4** Import Dialog



Import

Import Sources

Import from:

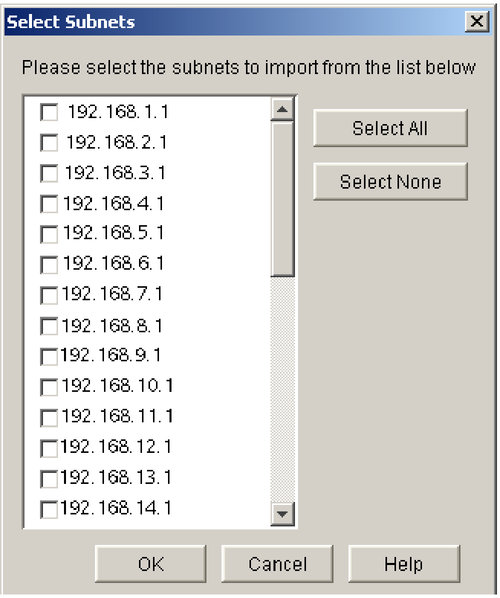
● HP OpenView

○ CSV File

*For information on how to import from a CSV file, see "Importing and Refreshing Devices" on page 87.*

**2** The *Import from HP OpenView* option is selected by default so click *OK* to display the *Select Subnets* dialog, which contains a list of subnets that HP OpenView has discovered. An example is shown in Figure 5:

**Figure 5** Select Subnets Dialog



Select Subnets

Please select the subnets to import from the list below

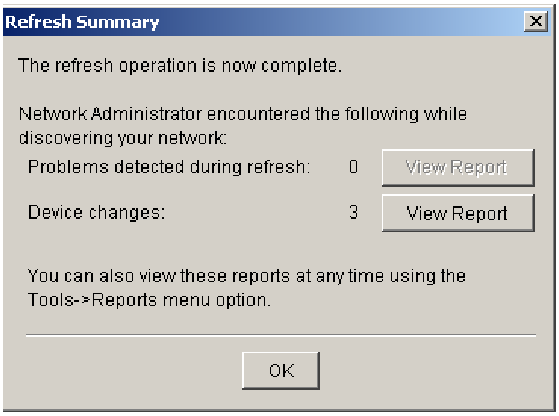
- □ 192.168.1.1
- □ 192.168.2.1
- □ 192.168.3.1
- □ 192.168.4.1
- □ 192.168.5.1
- □ 192.168.6.1
- □ 192.168.7.1
- □ 192.168.8.1
- □ 192.168.9.1
- □ 192.168.10.1
- □ 192.168.11.1
- □ 192.168.12.1
- □ 192.168.13.1
- □ 192.168.14.1

3 Select the subnets you want to import 3Com devices from and click *OK*.

An *Import Progress* dialog is displayed while 3Com Network Administrator contacts the HP OpenView database and retrieves device information for the 3Com devices in the subnets you have specified.

Once the import has taken place, the *Refresh Progress* dialog is displayed. During importing, 3Com Network Administrator (using SNMP) retrieves even more detailed information about your 3Com devices than is held in HP OpenView. When the refresh operation is complete, a *Summary* dialog is displayed as shown in Figure 6. From the *Summary* dialog you can view reports on the import and refresh operations.

**Figure 6** Summary Dialog



Refresh Summary

The refresh operation is now complete.

Network Administrator encountered the following while discovering your network:

Problems detected during refresh: 0

Device changes: 3

You can also view these reports at any time using the Tools->Reports menu option.

**4** Click *OK* to close the *Summary* dialog and return to the Device Window.

You are now ready to start using the administration functions of 3Com Network Administrator.

## Main Features

This section outlines the main features in 3Com Network Administrator, with references to the relevant chapters where each feature is described in more detail.

### Device Window

The 3Com Network Administrator Device Window is your console for viewing your 3Com devices. The window contains a tree view of device groups (called the *Device Group* tree) and a list of the devices in the selected groups (called the *Device List*). By using the Device Window, you are able to perform administration functions on specific devices, a selection of devices or entire device groups. A toolbar is included to provide access to the most commonly used administration tasks.

For more information, see “Device Window” on page 35.

## Device Administration

Whilst 3Com Network Administrator provides administration functions that apply to a range of your 3Com devices, you may want specific control of the details on a single device. For this reason, 3Com Network Administrator provides access to the following specific applications in order to obtain detailed control:

- Telnet Management
- Web Management
- 3Com Device View
- 3Com Switch Manager
- 3Com Router Manager
- Network Jack Configuration

3Com Network Administrator also includes a feature called Device Warranty. This feature enables you to register your 3Com devices for any applicable warranty.

For more information on the administration functions see "Device Administration" on page 61.

For more information on 3Com Device View, see Appendix B on page 251.

## Importing and Refreshing

Importing is a convenient way of retrieving just the 3Com devices from your HP OpenView database. You can also import information from a CSV file.

Refreshing is the term 3Com Network Administrator uses for retrieving detailed information from your 3Com devices. This information is then presented in the Device Window and in the reports that 3Com Network Administrator provides.

For more information, see "Importing and Refreshing Devices" on page 87.

## Backup, Restore and Setup

The Backup facility allows you to store the configuration of your devices. You can back up large numbers of devices and 3Com Network Administrator will store them on your computer.

The Restore facility allows you to select which configuration to restore to the device. You must have previously saved this configuration for the device.

If you have a number of devices with similar settings, you can use the Setup Wizard to deploy selected setup configurations to those 3Com devices.

For more information, see “Backup, Restore and Setup” on page 107.

## Agent Update

Agent Update allows you to update software on your 3Com devices if you have a valid support contract. Agent Update also works in conjunction with 3Com Network Administrator’s scheduling facility so that you can schedule the updates to take place overnight and minimize the impact on the network and, therefore, your users.

For more information, see “Agent Update” on page 135.

## Traffic Prioritization

Many 3Com devices have traffic prioritization (or quality of service) features. 3Com Network Administrator provides the Prioritize Network Traffic Wizard to simplify the configuration of these devices. Using the wizard, you can choose to prioritize or block specific servers or traffic types. To provide end-to-end quality of service, your configuration can be applied to all supported 3Com devices.

For more information, see “Prioritizing Network Traffic” on page 153.

## Reporting

The Reporting facility enables you to retrieve stored information about your 3Com devices. Many of the features in 3Com Network Administrator have their own reports but there are other, general purpose reports which give you different views of your 3Com devices. You can also create your own reports using the Custom Report facility.

For more information, see “Reporting” on page 191.

## HP OpenView Integration

3Com Network Administrator customizes your copy of HP OpenView with map icons and MIBs to enhance the management of your 3Com devices. It also integrates with the HP OpenView Event Browser to send you alarms for backup, restore, setup and agent update operations. Menu options are provided for you to be able to launch 3Com Network Administrator from within HP OpenView.

For more information, see "HP OpenView Integration" on page 209.

## Live Update

The Live Update feature keeps your copy of 3Com Network Administrator up-to-date with the latest device support and fixes. You can view and download updates specifically for your copy of 3Com Network Administrator. In addition, 3Com Product News is also available from Live Update to keep you informed with what is happening at 3Com.

For more information, see "Live Update" on page 221.

# 2 PRODUCT ACTIVATION

## Introduction

3Com Network Administrator uses an activation system which allows you to use your copy of the software beyond the grace period. This chapter describes how to activate 3Com Network Administrator.

Once you have installed 3Com Network Administrator, you can use it for a grace period of up to 60 days without activating it. During this time, you have the opportunity to activate the product each time you launch it.

It is important that you activate 3Com Network Administrator, this ends the grace period and allows you unrestricted access to the product. Activation also starts the product’s warranty period, entitling you to customer support for 3Com Network Administrator for the duration of the warranty. You can also decide to receive important update information relating to both this and other associated products.

This chapter covers the following topics:

## Key Concepts

3Com Network Administrator uses the following information in the activation process:

- The Serial Number — 3Com Network Administrator automatically generates this number when it is first installed.
- The License Key — identifies the physical copy of the software you have. Each 3Com Network Administrator CD has a unique license key.
- The Product Number — the part number of your software, which starts with '3C'.
  The part number for 3Com Network Administrator is 3C15400.
- The Activation Key — the key returned from the 3Com registration site. Type this key into the Activation Wizard to complete the activation process.

*3Com Network Administrator provides an Activation Wizard which guides you through the activation process.*

## Components

The following section describes how to activate 3Com Network Administrator.

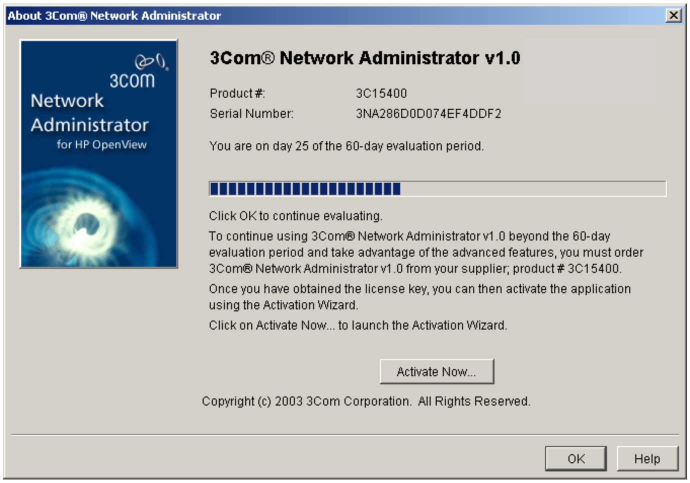
### About Dialog

3Com Network Administrator's About dialog is used to display general information relating to the product, such as the name, product number and serial number.

You can launch the About dialog by selecting the menu option *Help > About > 3Com Network Administrator.* If 3Com Network Administrator is still running within its grace period, the About dialog automatically displays each time the application is launched.

During the grace period, the About dialog displays the number of days remaining in the grace period. Click the *Activate Now...* button to launch the Activation Wizard as shown in Figure 7:

**Figure 7** About Dialog Before Registration



3Com® Network Administrator v1.0

Product #: 3C15400
Serial Number: 3NA286D0D074EF4DDF2

You are on day 25 of the 60-day evaluation period.

Click OK to continue evaluating.

To continue using 3Com® Network Administrator v1.0 beyond the 60-day evaluation period and take advantage of the advanced features, you must order 3Com® Network Administrator v1.0 from your supplier; product # 3C15400.

Once you have obtained the license key, you can then activate the application using the Activation Wizard.

Click on Activate Now... to launch the Activation Wizard.

Copyright (c) 2003 3Com Corporation. All Rights Reserved.

*When the grace period has expired, most menu options are disabled. However, you can still activate the product using the* Activate Now *menu option or by clicking* Activate Now *in the* About *dialog.*

You can close the dialog without activating the product by clicking *OK*.

*Once the product has been activated, the additional information and the* Activate Now *button will not be displayed.*

## Activation Wizard

The Activation Wizard guides you through the activation process. The Wizard can be launched either by clicking *Activate Now* on the About dialog, or by clicking *Help* > *Activate Now* from the top level menu.

Once 3Com Network Administrator is activated, the Activation Wizard is no longer needed and the *Activate Now* menu option displays a message box that confirms the product is activated instead.

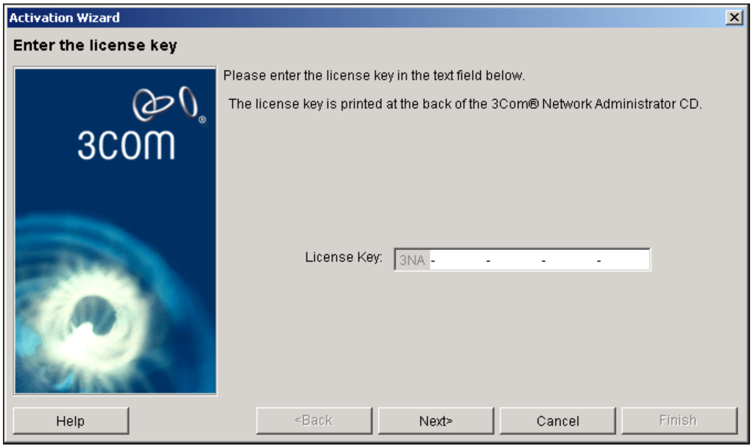
The wizard consists of two steps as follows:

1 Entering the license key — the key can be found on the CD sleeve of your 3Com Network Administrator software. The license key is five groups of hexadecimal characters separated by dashes. For example:

3NA - 1BF9 - 093B - AC5F - 8343

Type the license key into the *License Key* text box and click *Next* as shown in Figure 8:

**Figure 8** Activation Wizard - License Key



Activation Wizard

**Enter the license key**

Please enter the license key in the text field below.

The license key is printed at the back of the 3Com® Network Administrator CD.

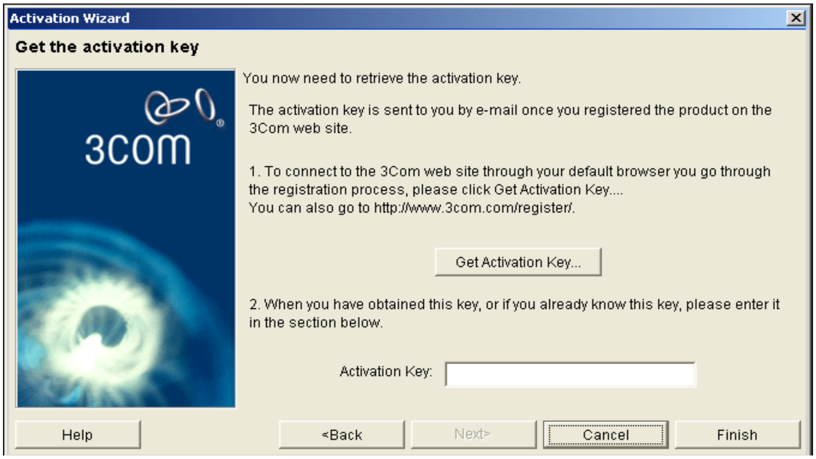
License Key: 3NA - - - -

3Com Network Administrator checks that you have a valid license key before allowing you to continue.

**2** Obtaining the activation key — the activation key step allows you to do two things:

- Connect to the 3Com registration web site by clicking *Get Activation Key*.
- Enter the activation key you receive from the 3Com web site by typing it in to the *Activation Key* text box and clicking *Finish* in the wizard as shown in Figure 9:

**Figure 9** Activation Wizard - Activation Key



Activation Wizard

**Get the activation key**

You now need to retrieve the activation key.

The activation key is sent to you by e-mail once you registered the product on the 3Com web site.

1. To connect to the 3Com web site through your default browser you go through the registration process, please click Get Activation Key....
You can also go to http://www.3com.com/register/.

2. When you have obtained this key, or if you already know this key, please enter it in the section below.

Activation Key:

*The wizard already knows the product number and serial number so you do not have to type them in.*

To obtain the activation key for this copy of 3Com Network Administrator, click *Get Activation Key*. This launches your default web browser, which displays the 3Com registration web site. 3Com Network Administrator sends the serial number, product number and license key for you. Follow the instructions on the web site to complete the product registration process. Once registration is complete, the web site displays your activation key. You will also be sent a copy of this key via e-mail.

*If you prefer, you can register your product manually at:*

```
http://www.3com.com/register
```

*However, 3Com recommends that you use the Activation Wizard.*

## Examples

The following section provides an example of using the Activation process.

### Activating 3Com Network Administrator

You have installed 3Com Network Administrator on your computer and you want to activate it.

**1** Start 3Com Network Administrator. The *About* dialog will appear, showing the number of days remaining in the grace period.

**2** In the *About* dialog, click *Activate Now* to display the Activation Wizard.

**3** Enter the license key (as printed on the product's packaging) in the *License Key* text box and click *Next*.

If the license key is valid, the wizard moves to the *Activation Key* step.

**4** From the *Activation Key* step, click *Get Activation Key.* Your default web browser is launched which automatically directs you to the 3Com registration site.

If the wizard fails to launch your web browser, you can go directly to 3Com's registration system by opening your preferred web browser and entering the following URL into the browser's address bar:

```
http://www.3com.com/register
```

**5** Follow the instructions on the registration site to complete the registration of the product and obtain the activation key. 3Com will also send you a copy of your activation key via e-mail.

6 Enter the activation key in the *Activation Key* text box to activate the product.

## Useful Information and References

The following section provides useful information and references when activating 3Com Network Administrator.

### Where can I find the product number for 3Com Network Administrator?

The product number for 3Com Network Administrator is found on the the product's packaging and is also displayed in the About dialog. To launch the About dialog, select *Help > About > 3Com Network Administrator* from the menu on the main window.

### Where can I find the serial number for 3Com Network Administrator?

The serial number for your copy of 3Com Network Administrator is displayed in the About dialog.

### Where can I find the license key for 3Com Network Administrator?

The license key is printed on a card inside the 3Com Network Administrator packaging. If you are using an evaluation copy downloaded from the 3Com web-site, you cannot activate the product. Please contact your preferred 3Com reseller to buy a copy of the product as a physical shipment.

## Key Considerations

The following section provides useful information when activating 3Com Network Administrator.

### What if I lose my Activation Key after registration?

You can re-register your copy of 3Com Network Administrator to obtain your activation key again. You will also receive an e-mail confirmation of your activation key.

When you are re-registering the product, it is very important to enter exactly the same user and product information during the original registration. This includes the username, product number, serial number, and license key. Entering different information may result in the registration begin rejected.

### How do I move my copy of 3Com Network Administrator to another workstation?

If you need to move 3Com Network Administrator to another computer, you must contact 3Com Customer Support to revoke the existing activation key. The activation key will only work with the correct combination of license key (to identify the software) and serial number (to identify the machine the software is installed on). To comply with the software license agreement you must remove the original installation.

### If I re-install the product after it has been activated, do I need to activate it again?

No - the product activation information is stored on your computer and will remain intact following de-installation and re-installation.

### My copy of 3Com Network Administrator no longer runs, even though it has been activated.

If you upgraded a major component on your computer, such as the processor, or hard disk driver or if you upgrade your computer's operating system, the serial number will then be invalid. In this case, you need to contact 3Com Customer Support to have your activation key revoked. Refer to "How do I move my copy of 3Com Network Administrator to another workstation?" above for more information.

### Why can't I log in to the 3Com support web site?

If you experience difficulties logging in to the 3Com support web site, please check your web browser settings to ensure that cookies are enabled. You may also want to check with your system administrator that your site's firewall settings permit web site cookies.

# 3 DEVICE WINDOW

## Overview

This chapter describes the 3Com Network Administrator device window. The device window provides a view of the 3Com devices on your network, and arranges them into groups. These groups are displayed in a tree on the left side of the window. Devices in the selected group are displayed in a list on the right side of the window. All of the features in 3Com Network Administrator are accessed from the device window.

This chapter covers the following topics:

- Key Concepts
- Components
- Examples
- Key Considerations

## Key Concepts

This section describes the 3Com Network Administrator key concepts relating to the device window.

### Inventory Files

3Com Network Administrator stores device information in inventory files. Inventory files have the file extension ‘`.inv`'. They are exclusive to 3Com Network Administrator and are not related to HP OpenView.

Only one inventory file may be open at any one time. Opening a new inventory file will close the current inventory file.

All operations invoked from 3Com Network Administrator are applied to the current inventory file. For example, importing data from either HP OpenView or a CSV file results in the current inventory file being updated with the newly gathered information. 3Com Network Administrator does not alter the CSV files or HP OpenView maps it imports device information from.

Two other types of files are saved alongside inventory files. These files use the same name as the inventory file but have `.mdb` and `.properties` file extensions. These files are used internally by 3Com Network Administrator. Whilst the presence of these files is not required to successfully load an inventory file, some user-defined options may not be set if they are not present.

### Device Groups

Device Groups are displayed on the left side of the device window.

There are two main groups in the Device Group Tree:

- All 3Com Devices
- Standard Groups

The purpose of these groups is explained as follows:

### All 3Com Devices Group

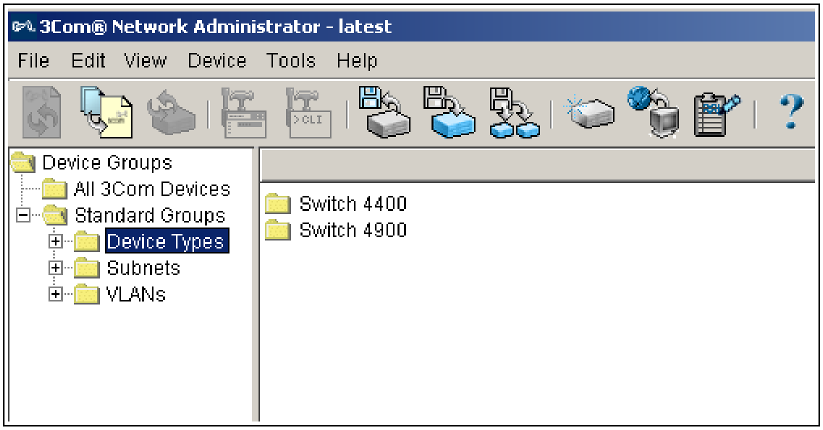
This group displays all 3Com devices present within the currently open inventory file. You should use this when you want to perform operations on all the devices in the current inventory file.

### Standard Groups

This group contains sub-groups based on the type of devices present in your inventory file. The sub-groups are:

- **Device Types** — if your inventory contained 3Com SuperStack® 3 Switch 4400s and SuperStack 3 Switch 4900s for example, there would be two sub-groups present within the 'Device Types' group. An example is shown in Figure 10.

**Figure 10** Device Types Group

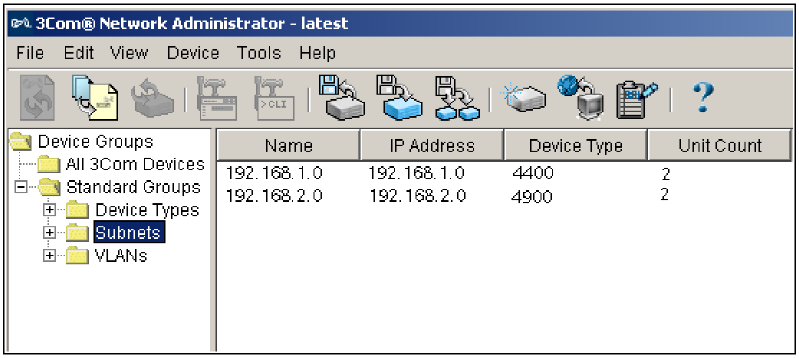


The device type name is shortened to make navigating the tree more convenient. For example, '3Com SuperStack 3 Switch 4900' is shortened to 'Switch 4900'. All sub-groups listed under the 'Device Types' group are sorted alphabetically, then numerically.

- **Subnets Group** — this group contains sub-groups based on the IP address and subnet mask of the devices present in your inventory file. Each Subnets group is named using the network address of the subnet, followed by the subnet mask.

  For example, if the devices in your inventory file are on the following networks: 192.168.1.0 (255.255.255.0) and 192.168.2.0 (255.255.255.0), there will be two sub-groups present under the 'Subnets' group. An example is shown in Figure 11.

**Figure 11** Subnets Group



| Name | IP Address | Device Type | Unit Count |
|---|---|---|---|
| 192.168.1.0 | 192.168.1.0 | 4400 | 2 |
| 192.168.2.0 | 192.168.2.0 | 4900 | 2 |

  All sub-groups listed under the 'Subnets' group are sorted according to network address.

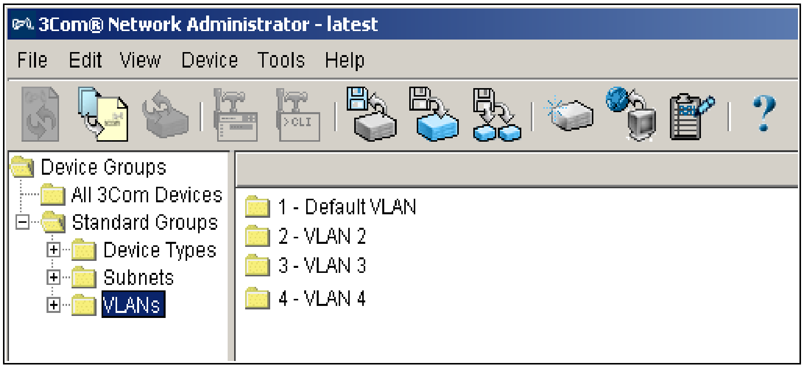
- **VLANs Group** — this group contains sub-groups based on the VLAN membership of the devices in your inventory file. Each VLAN sub-group is named using the VLAN ID followed by the VLAN name.

  For example, if some devices present in your inventory are members of VLAN 1, named 'Marketing' and other devices present are members of VLAN 2, named 'Accounting', the sub-groups ‘1 - Marketing’ and ‘2 - Accounting’ would be present in the VLANs Group.

A VLAN sub-group is considered unique if it has a unique VLAN ID and a unique name. The name is case sensitive, so a VLAN named 'marketing', with a lowercase 'm', is considered different to a VLAN named 'Marketing', with an uppercase 'M'. VLANs with the same ID and name on either side of a router are considered to be the same VLAN for the purposes of the VLANs group.

Devices with no available VLAN information are added to a specific 'Undetermined' VLAN sub-group as shown in Figure 12.

**Figure 12** VLAN Groups



All sub-groups listed under the 'VLANs' group are sorted first by VLAN ID, then by VLAN name. If the 'Undetermined' sub-group is present, it is added as the first group in the VLANs group.

## Components

The following section describes the features of the Device Window and describes the operations you can perform from this window.

### The Device Group Tree

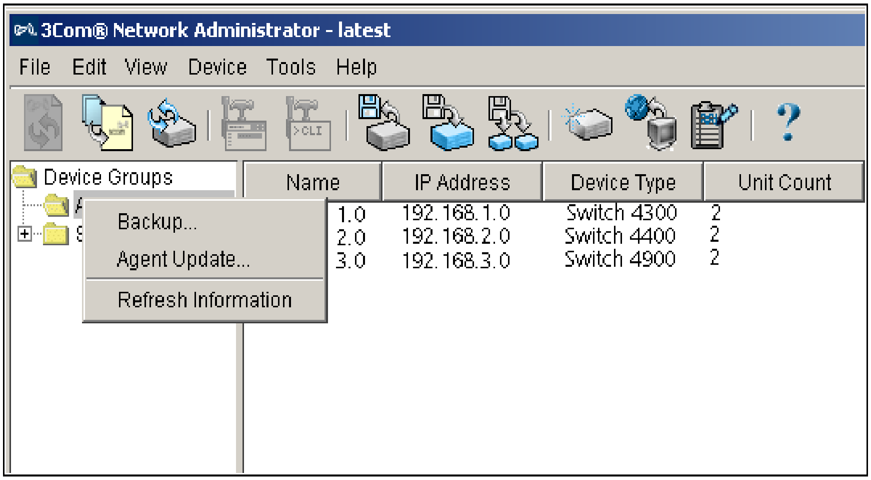
The device group tree is located on the left side of the 3Com Network Administrator device window.

#### Device Group Tree Right-click Menus

A right-click menu is available for a device group by right-clicking on the required group. Only one device group may be selected at a time. Right-click menus can only be applied to sub-groups or to groups that contain no sub-groups. Such groups include the 'All 3Com Devices' group and any of the sub-groups under 'Standard Groups' (that is, 'Device Types', 'Subnets' and 'VLANs' groups). Right-clicking on 'Standard Groups' or any of its sub-groups will not produce a right-click menu.

The options available in the right-click menu are shown in Figure 13.

**Figure 13** Group Tree Right-click Menu



| Name | IP Address | Device Type | Unit Count |
|---|---|---|---|
| 1.0 | 192.168.1.0 | Switch 4300 | 2 |
| 2.0 | 192.168.2.0 | Switch 4400 | 2 |
| 3.0 | 192.168.3.0 | Switch 4900 | 2 |

Selecting an item in the right-click menu performs the corresponding operation for all of the devices within the selected group or sub-group.

The operations available in the right-click menu are equivalent to corresponding menu items in the main menu. Please refer to "Menus" on page 44 for more information.

## The Device List

The device list shows the devices contained within a device group. Selecting a device group in the device group tree displays the devices within the group in the device list.

Multiple selection is allowed in the device list and is achieved through either of the following:

- Holding down a mouse button and dragging over a selection of devices in the list.
- Clicking on different devices while holding down the CTRL or SHIFT keyboard buttons.

## Device List Columns

The following columns are available in the device list:

- **Name** — the name of the device, as specified in HP OpenView or the CSV file.
- **IP Address** — the IP Address of the device.
- **Device Type** — the type of device, for example, Switch 4400, Switch 4900, Switch 4060.
- **Unit Count** — the number of units in the device's stack or chassis. Devices that are not stacked display '1' in this column. If there is no unit information the column is left blank.
- **SNMP Read Community** — the read community string that 3Com Network Administrator is using to communicate with the device.
- **SNMP Write Community** — the write community string that 3Com Network Administrator is using to communicate with the device.
- **Subnet** — the subnet mask of the device.
- **Contact** — the contact name for the device, taken from the sysContact MIB variable.
- **Location** — the location name for the device, taken from the sysLocation MIB variable.

When the application is run for the first time, only the default columns (Name, IP Address, Device Type and Unit Count) are displayed.

Columns can be resized by dragging either edge of a column header to a new position. Columns can be reordered by dragging a column header to a new location. Any changes made are applied to all device groups.

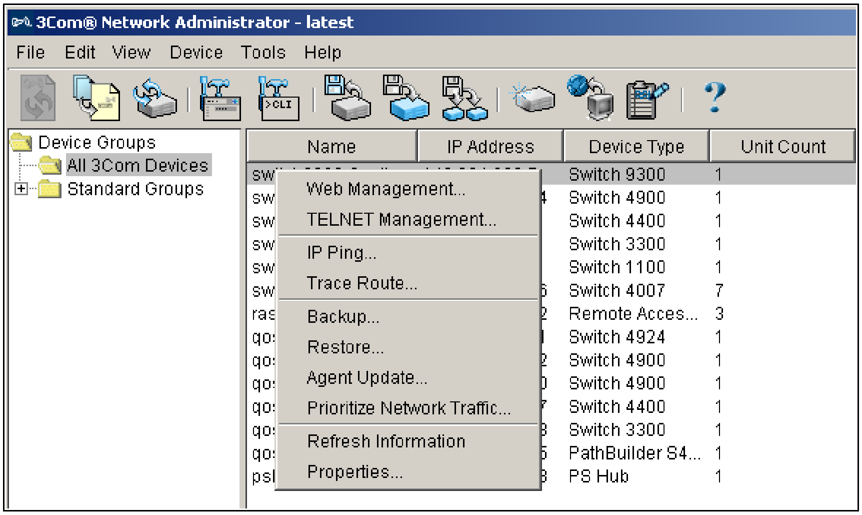
You can sort the entire list using the information in a given column by clicking on its column header. Initially the list is sorted by the left-most column.

You can add or remove columns from the device list using the *Show Columns* dialog. Please refer to "View > Show Columns" on page 52 for more information.

### Device List Right-click Menus

Selecting a device in the device list and right clicking on it launches a right-click menu. This is shown in Figure 14.

**Figure 14** Device List Right-click Menu



| Name | IP Address | Device Type | Unit Count |
|---|---|---|---|
| sw |  | Switch 9300 | 1 |
| sw | 4 | Switch 4900 | 1 |
| sw |  | Switch 4400 | 1 |
| sw |  | Switch 3300 | 1 |
| sw |  | Switch 1100 | 1 |
| sw | 6 | Switch 4007 | 7 |
| ras | 2 | Remote Acces... | 3 |
| qo | 1 | Switch 4924 | 1 |
| qo | 2 | Switch 4900 | 1 |
| qo | 0 | Switch 4900 | 1 |
| qo | 7 | Switch 4400 | 1 |
| qo | 3 | Switch 3300 | 1 |
| qo | 5 | PathBuilder S4... | 1 |
| psl | 3 | PS Hub | 1 |

Multiple selection is possible within the device list. However, not all items in the right-click menu can be applied to multiple selections. In this case, any such items in the menu are omitted.

The operations provided by the right-click menu are equivalent to corresponding menu items in the main menu. Please refer to "Menus" on page 44 for more information.

## Toolbar

The toolbar provides access to the most commonly used administration tools.

Some items in the toolbar are not applicable to multiple or group selection. When this is the case, the toolbar button is grayed out.

Hovering the mouse cursor over a button in the toolbar causes a 'tooltip' for that button to be displayed. The tooltip describes the operation associated with the button.

The operations provided by the toolbar buttons are equivalent to their corresponding menu items. Please refer to the "Menus" on page 44 for more information.

## Status Bar

The status bar provides detailed information about items within the device window, as well as providing a location for minimized progress dialogs such as the *Refresh Progress* dialog.

The status bar provides information on the current selection as follows:

- For a selected group in the Device Group Tree the text displayed is:

  `Selected Group <Group Name>. Contains <number selected> items.`

- For a single selected device in the device list the text displayed is:

  `Selected device <Device Display Name>`

- For multiple device selection in the device list the text displayed is:

  `Selected <number selected> items.`

*This information is useful if you need to count the number of devices with a given property. For example, if you need to know how many devices are in VLAN 1 — 'Marketing', simply select the appropriate VLANs sub-group in the device group tree. The status bar text displays how many devices are in that group.*

The status bar also provides detailed information about a menu item when it is highlighted.

## Menus

Table 4 lists each menu item for a given main menu and the associated operation invoked by selecting it.

**Table 4** File Menu

| Menu Item | Hot Key | Operation |
|---|---|---|
| New | Ctrl+N | Creates a new empty inventory file. Prompts for a save if the current inventory has changed. See "File > Open" on page 48 for more information. |
| Open | Ctrl+O | Opens an existing inventory file. Prompts for a save if the current inventory has changed. See "File > Open" on page 48 for more information. |
| Save | Ctrl+S | Saves the current inventory file. Prompts for a filename if the inventory has not been saved previously. See "File > Save and Save As" on page 48 for more information. |
| Save As… | | Saves the current inventory file using a specified name. See "File > Save and Save As" on page 48 for more information. |
| Import… | | Launches the Import dialog used to import CSV and HP OpenView device information. See "Importing and Refreshing Devices" chapter on page 87 for more information. |
| Most Recently Used File List | | See "Most Recently Used Files" on page 49 for more information. |
| Exit | | Exits 3Com Network Administrator. Prompts for a save if the current inventory has changed. See "File > Exit" on page 49 for more information. |

**Table 5** Edit Menu

| Menu Item | Hot Key | Operation |
|---|---|---|
| Add Device… | | Launches the Add Device dialog. This dialog allows you to add a new device to the inventory file. See "Edit > Add Device" on page 49 for more information. |
| Delete | Ctrl+Delete | Deletes the selected device. See "Edit > Delete" on page 50 for more information. |
| Find… | Ctrl+F | Launches the Find dialog. This dialog allows you to find devices by Name, User Name, IP or MAC address, Device Type or VLAN. See "Edit > Find" on page 51 for more information. |
| Select All | Ctrl+A | Selects all devices in the Device Window. See "Edit > Select All" on page 52 for more information. |

**Table 6** View Menu

| Menu Item | Hot Key | Operation |
|---|---|---|
| Show Toolbar | | Toggles whether the toolbar is displayed or not. See "View > Show Toolbar" on page 52 for more information. |
| Show Columns… | | Launches the Show Columns dialog. This dialog allows you to add or remove columns from the device list. See "View > Show Columns" on page 52 for more information. |
| Update Window | | Updates the inventory with data received after a scheduled refresh. See "View > Update Window" on page 53 for more information. |

**Table 7** Device Menu

| Menu Item | Hot Key | Operation |
|---|---|---|
| Web Management… | | Launches the web interface for the selected device. |
| Telnet Management… | | Launches the Telnet management interface for the selected device. |
| Backup… | | Launches the Backup wizard for the selected devices. See "Device Backup Wizard" on page 109 for more information. |
| Restore… | | Launches the Restore wizard for the selected device. See "Device Restore Wizard" on page 114 for more information. |
| Setup… | | Launches the Setup wizard. See "Device Setup Wizard" on page 119 for more information. |
| Agent Update… | | Launches the Agent Update wizard for the selected devices. See "Agent Update Wizard" on page 137 for more information. |
| Agent Import… | | Launches the Agent Import dialog. See "Import Dialog" on page 92 for more information. |
| Refresh Information | | Updates the information for the selected devices. See "Refreshing" on page 90 for more information. |
| Properties… | | Launches the Properties dialog for the selected devices. See "Importing and Refreshing Devices" on page 87 for more information. |

**Table 8** Tools Menu

| Menu Item | Hot Key | Operation |
|---|---|---|
| Reports… | | Launches the Reports dialog. See "Reports Dialog" on page 197 for more information. |
| Prioritize Network Traffic… | | Launches the Prioritize Network Traffic wizard. See "Prioritize Network Traffic Wizard" on page 161 for more information. |
| Device Warranty… | Ctrl+W | Launches the Device Warranty wizard. See "Device Warranty Wizard" on page 72 for more information. |
| Scheduled Tasks… | | Launches the Scheduled Tasks dialog, where all currently scheduled tasks are listed. See "Tools > Scheduled Tasks" on page 53 for more information. |
| Live Update… | | Launches the Live Update wizard. See "Live Update Setup Wizard" on page 223 for more information. |
| Options… | | Launches the Options dialog. See "Tools > Options" on page 55 for more information. |

**Table 9** Help Menu

| Menu Item | Hot Key | Operation |
|---|---|---|
| Contents and Index… | | Launches the online help. See "Help > Contents and Index" on page 58 for more information. |
| Register Now… | | Launches the Registration dialog. See "Getting Started" on page 17 for more information. |
| About… | | Launches the About dialog. See "Help > About" on page 58 for more information. |

## File > Open

The *File* > *Open* option is used to open an inventory (.inv) file for use within 3Com Network Administrator.

The default directory for opening inventory files is:

```
<3Com Network Administrator install dir>\inventory_files
```

The default directory may be changed using the *Options* dialog, for more information see "Tools > Options" on page 55.

Once the inventory file has been located, select it and click *OK*. This loads the inventory file into 3Com Network Administrator. To abort the open operation click *Cancel* to return to the Device Window.

Opening a new inventory file when another inventory file is currently open causes the new file to be loaded in place of the currently open file. If the current inventory file contains any unsaved changes, you are prompted to save the file. Cancelling this operation returns you to the current inventory file without any changes being made.

If you re-open the current inventory file, the open operation will not take place if there are no saved changes in the current file. If, however, the current inventory file has changed, you are prompted on whether you wish to revert to the saved inventory file.

## File > Save and Save As

The *File* > *Save* and *Save As* operations are used to save the current inventory file. The Save operation saves the currently loaded inventory file using the current file name. If the inventory file is untitled, the Save operation will launch the *Save As* dialog.

The *Save As* operation is used to save an inventory using a specified filename, typed into the *File name* text field.

The default directory for saving inventory files is:

```
<3Com Network Administrator install dir>\inventory_files
```

The default location may be changed using *Tools* > *Options*, for more information see "Tools > Options" on page 55.

To save an inventory file in a different directory to the default location, use the *Save As* dialog's browser to select the directory where the inventory file is to be saved. Click *Save* to save the file.

Click *Cancel* if you wish to abort the Save operation. This returns you to the Device Window.

### Most Recently Used Files

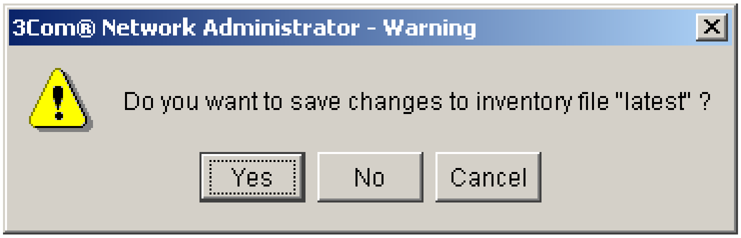
In the *File* menu, between the *Import* and *Exit* menu items, is a list of the last four inventory files that you have been using. This list is called the Most Recently Used (MRU) file list, and is updated every time you open or save an inventory file.

To open one of the inventory files in the MRU file list, select the appropriate item in the *File* menu or use the Hot Keys Ctrl+1 to Ctrl+4.

### File > Exit

This operation closes 3Com Network Administrator. The following message will display if there are outstanding changes to the inventory that need to be saved:

**Figure 15** Closing 3Com Network Administrator



3Com® Network Administrator - Warning

Do you want to save changes to inventory file "latest" ?

*Any scheduled tasks present in the Scheduled Tasks list are cancelled when the application closes.*

### Edit > Add Device

This dialog is used to add a device to the current inventory file by manually entering information about the device into the dialog.

- **Name** — the name of the device that is displayed in the inventory file.
- **IP Address** — the IP Address of the device to be added to the inventory.
- **Read** — the SNMP read community string used to communicate with this device.
- **Write** — the SNMP write community string used to write to this device.

Compulsory fields are the IP Address and the Read Community String. If you do not enter information into these fields, a warning message is displayed when *OK* is clicked. You are returned to the *Add Device* dialog to enter the required information.

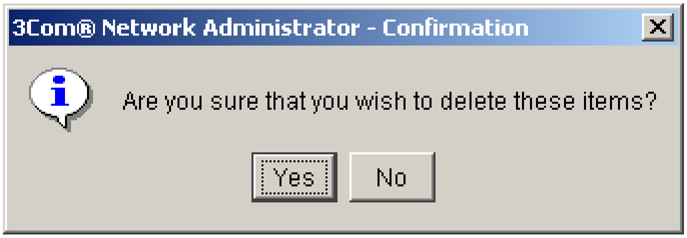
If a device is added successfully to the current inventory, a message dialog informs you that the operation was successful.

*The* Add Device *dialog is not available while a refresh operation is in progress.*

## Edit > Delete

Deleting a device from any group within 3Com Network Administrator removes it from the entire inventory file. The device is removed from all device groups when you click *Yes* on the confirmation dialog as shown in Figure 16.

**Figure 16** Deleting a Device



3Com® Network Administrator - Confirmation

Are you sure that you wish to delete these items?

Multiple devices may be deleted at the same time by highlighting them in the device list and selecting *Edit > Delete.*

If as a result of a delete operation a group is then empty, that group is removed from the device group tree unless the group is one of the 'Standard Groups' or the 'All 3Com Devices' group.

### Edit > Find

The *Find* dialog is used to search for devices within your inventory according to the criteria listed in Table 10. To change the search criteria simply select the appropriate item in the 'Search By' list.

**Table 10** Search criteria for finding devices within an inventory

| **Search Criteria** | **Description** |
|---|---|
| Name | Enter the name of the device to search for in the supplied 'Name' text field. |
| IP Address | Enter the IP Address of the device to search for in the supplied 'IP Address' field. |
| MAC Address | Enter the MAC address of the device to search for in the supplied 'MAC Address' field. |
| Device Type | Select the type of device, e.g. SuperStack 3 Switch 4400, to search for in the supplied 'Device Type' combo box. |
| VLAN | Select the VLAN name and ID to search for in the supplied 'VLAN' combo box. |

*Wildcards (* and ?) are allowed within search strings:*

** - Matches 0 or more characters.*
*? - Matches a single character.*

Devices that match the search criteria are added to the results list. The number of matches is displayed in the *Find* dialog's status bar. Items in the results list may be selected and the following pull right options are available for them:

- Web Management
- Telnet Management
- IP Ping...
- Trace Route...
- Backup…
- Restore…
- Agent Update…
- Prioritize Network Traffic…
- Refresh Information…
- Properties…

For more information on these menu items refer to "Menus" on page 44.

### Edit > Select All

This option selects all of the devices in the currently selected group. For a device list containing no devices, the *Select All* option is grayed out.

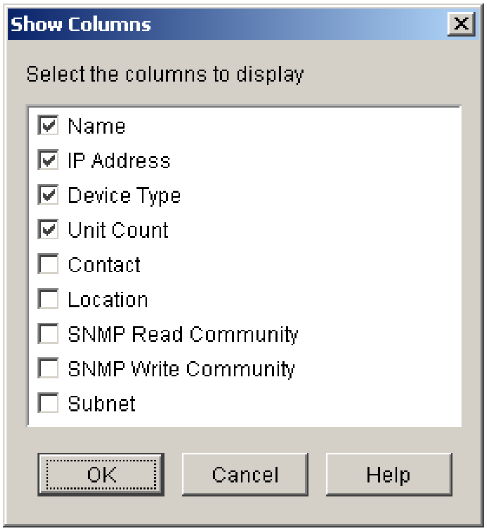
### View > Show Toolbar

This menu item toggles between a visible or hidden toolbar. If you find you do not use the toolbar, hiding it provides more space for the device group tree and device list.

### View > Show Columns

This menu item launches the *Show Columns* dialog. This dialog is used to add and remove columns from the device list as shown in Figure 17:

**Figure 17** Show Columns Dialog



Show Columns

Select the columns to display

- ☑ Name
- ☑ IP Address
- ☑ Device Type
- ☑ Unit Count
- □ Contact
- □ Location
- □ SNMP Read Community
- □ SNMP Write Community
- □ Subnet

To add a column, simply check the appropriate check box. To remove a column, uncheck the appropriate check box. Click *OK* to update the device list and display the selected columns.

You can have no columns selected, but the application warns you that no information will be displayed in the device list.

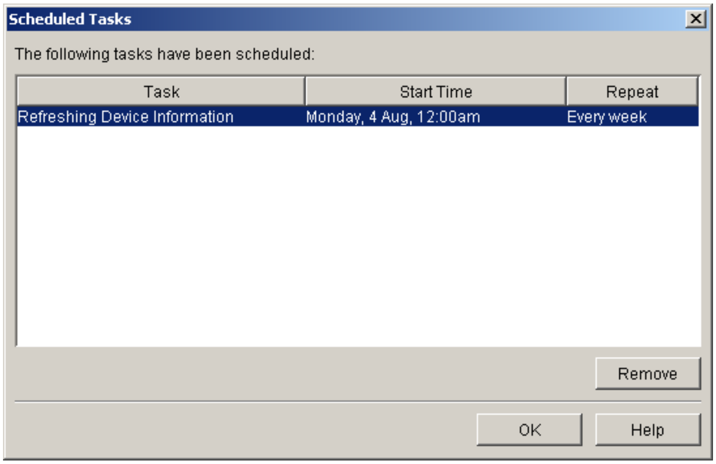
### View > Update Window

This menu item is enabled when there is some pending information to be added to the inventory. This occurs after a scheduled refresh has completed. Selecting this option adds the newly refreshed information to the inventory file.

### Tools > Scheduled Tasks

This menu item launches the *Scheduled Tasks* dialog as shown in Figure 18:

**Figure 18** Scheduled Tasks



Scheduled Tasks

The following tasks have been scheduled:

| Task | Start Time | Repeat |
|---|---|---|
| Refreshing Device Information | Monday, 4 Aug, 12:00am | Every week |

The *Scheduled Tasks* dialog displays a list of all currently scheduled tasks. Operations that may be scheduled include Device Backup, Agent Update and Refresh. Each task has a name, a start time and how often the task repeats (if applicable). For tasks that are not repeatable, for example, the backup operation, the *Repeat* column displays *N/A*.

Only one scheduled task can run at a given time. If two or more tasks are set to run at the same time, the first task is executed and all others enter a 'pending' state (the *Start Time* column displays *Pending)*. The pending task is executed immediately after the currently scheduled task finishes.

A scheduled task also enters the pending state if it is scheduled to start but cannot for some reason. For example, if a manual refresh is currently in progress which prevents a scheduled refresh from executing. Once the blocking task has finished the pending scheduled task is executed.

If the following scheduled tasks are running:

- Agent Update
- Backup
- Restore
- Setup
- Prioritize Network Traffic
- Refresh

Then:

- The following operations are prohibited from running:
  - File > New
  - File > Open
  - Edit > Add Device
  - Edit > Delete
  - Device > Refresh Information
  - Tools > Prioritize Network Traffic
- The following tasks are not blocked if they are currently running:
  - Agent Update
  - Backup
  - Restore
  - Setup

  Instead you are given the choice of:
  - Queuing the new task to run after the current task finishes.
  - Cancelling the current task, allowing the new task to run immediately.
  - Cancelling the new task, allowing the current task to finish.

*For scheduled tasks to execute, 3Com Network Administrator must be running. On exiting the application all currently scheduled tasks are cancelled.*

## Tools > Options

This menu item launches the *Options* dialog, which is used to configure the default behavior of 3Com Network Administrator. The *Options* dialog consists of four tabs:

- **General** — default file locations and how the application should behave.
- **Device Management** — options for managing devices in your inventory.
- **Internet** — how 3Com Network Administrator should connect to the internet.
- **Refresh** — refresh options available to 3Com Network Administrator.

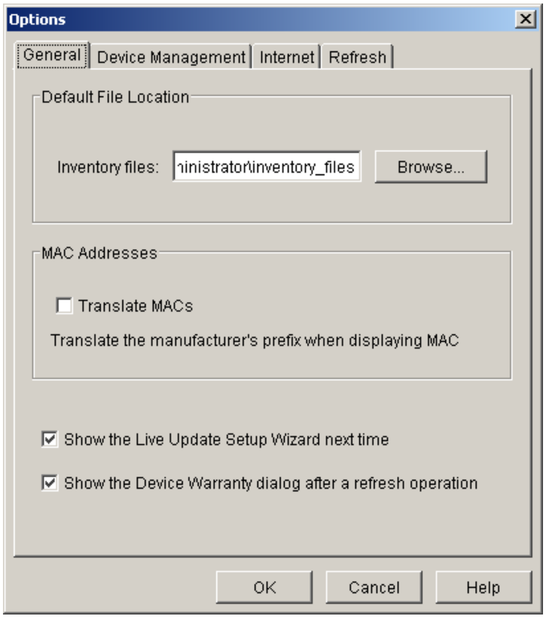
### General

This tab (as shown in Figure 19) displays the following:

- **Default File Location** — change the default *inventory files* location to a different location. Click *Browse* to choose the directory you want. If the path you enter does not exist, you are warned of this when you click *OK*.

  The default directory is: `<3Com Network Administrator install dir>\inventory_files`.

**Figure 19** General Tab



Default File Location

Inventory files: ninistrator\inventory_files

MAC Addresses

□ Translate MACs

Translate the manufacturer's prefix when displaying MAC

☑ Show the Live Update Setup Wizard next time

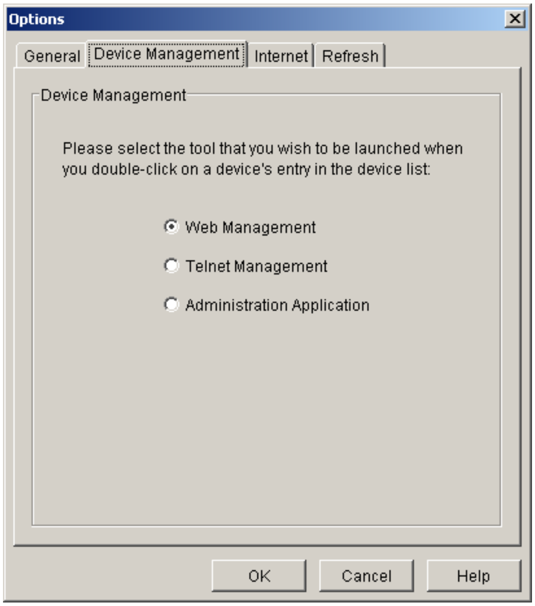
☑ Show the Device Warranty dialog after a refresh operation

- **MAC Addresses** — for any MAC address displayed, you can append the manufacturers name to the start. For example, 00-c0-00-xx-xx-xx becomes 3Com-xx-xx-xx. This option is disabled by default.
- **Show the Live Update Setup Wizard next time** — this option is enabled by default (see "Live Update Setup Wizard" on page 223 for more information).
- **Show the Device Warranty dialog after a refresh operation** — this is enabled by default.

### Device Management

This tab allows you to change the management application that is launched when a device is double clicked in the list as shown in Figure 20:

**Figure 20** Device Management Tab



Please select the tool that you wish to be launched when you double-click on a device's entry in the device list:

● Web Management

○ Telnet Management

○ Administration Application

Choose from the Web Management (default), Telnet Management or Administration Application. If a device does not support the preferred Web Management application, Telnet is launched instead.

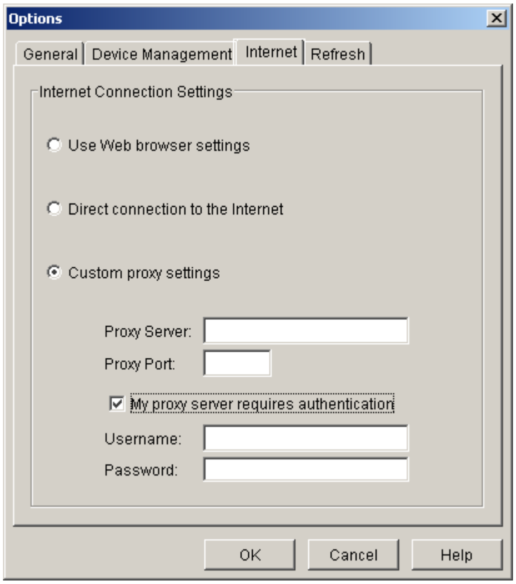
*For further information on the Device Management options see "Device Administration" on page 61.*

### Internet

This tab (as shown in Figure 21) allows you to select one of the following options:

- **Use Web browser settings** — this is the default option. If your web browser uses a proxy server to access the internet, 3Com Network Administrator will use the same system.

**Figure 21** Internet Tab



Internet Connection Settings

○ Use Web browser settings

○ Direct connection to the Internet

● Custom proxy settings

Proxy Server:

Proxy Port:

☑ My proxy server requires authentication

Username:

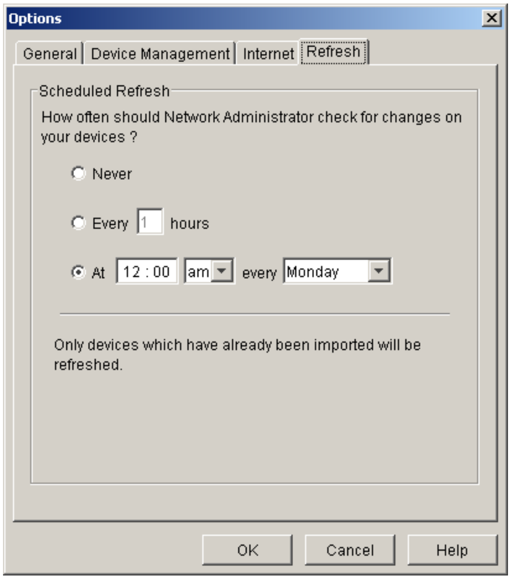
Password:

- **Direct connection to the Internet** — use this option if your management station connects to the Internet directly through a Local Area Network, without using a proxy server.
- **Custom proxy settings** — specify the URL to the proxy server followed by the proxy port number. If your proxy server requires authentication click the *My proxy server requires authentication* check box and enter the username and password.

### Refresh

This tab (as shown in Figure 22) allows you to schedule refresh operations to repeat at specified times. Select from repeating every x hours or at a specific time every day, weekday, or week. For further information on the Refresh tab see "Delaying Refreshing Existing Devices" on page 100.

**Figure 22** Refresh Tab



Scheduled Refresh

How often should Network Administrator check for changes on your devices ?

○ Never

○ Every 1 hours

● At 12 : 00 am every Monday

Only devices which have already been imported will be refreshed.

### Help > Contents and Index

This launches the Contents and Index pages of the online help.

### Help > About

When you launch 3Com Network Administrator for the first time, the *About* dialog is displayed.

The dialog shows the product name, product number, serial number and the major version number. Any service packs installed are also listed.

## Examples

The following section contains useful examples on using the Device Window.

### Finding the IP address of a Device

You have discovered that a particular MAC address is causing problems on your network. You want to know the name and IP address of the device causing the problem, given its MAC address:

**1** Launch the *Find* dialog, using *Edit* > *Find* or *CTRL+F*.

**2** Change the *Search By* combo box option to *MAC Address*.

**3** Type the known MAC address into the MAC Address field provided.

**4** Click *Find*. The device with the corresponding MAC address is displayed in the results list.

The IP address of the device is listed in the results list.

### Backing up Devices in a certain VLAN

You are about to upgrade the agent software on the switches in VLAN 5 (your Accounts department VLAN). Before you do, you want to back up their software configurations. To do this:

**1** Launch the *Find* dialog, using *Edit* > *Find* or *CTRL+F*.

**2** Change the *Search By* combo box option to *VLAN*.

**3** Set the VLAN to search for *(ID=5) Accounting Department* VLAN.

**4** Click *Find*. The devices matching the selected VLAN appear in the results list. Select all of the devices in the list and right-click on them.

**5** Select *Backup* from the right-click menu.

**6** Complete all the wizard steps to upgrade the appropriate devices.

*You could also perform this operation by selecting 'VLAN 5' in the device group tree and selecting* Device Backup*.*

### Adding a New Device

A new 3Com device has been added to your network with the IP address 192.168.1.1. The location of the device is in Building 1, Rack 4. The name of the device is b1r4-192.168.1.1. The SNMP read community string has been set to be netman2003r, the write SNMP community string has been set to be netman2003w.

To add this device to the current inventory file, use the *Add Device* dialog as follows:

1. Launch the *Add Device* dialog using the *Edit* > *Add Device* menu option.
2. Enter the name of the device into the *Name* field as **`b1r2-192.168.1.1`**.
3. Enter the IP address of the device into *IP Address* field as **`192.168.1.1`**
4. Enter the read community string into the *Read* text field as **`netman2003r`**.
5. Enter the write community string into the *Write* text field as **`netman2003w`**.
6. Click *OK*.

   If all information has been entered correctly an information dialog appears, stating that the new device has been added successfully.
7. Click *OK* to close the dialog.

   The new device is now listed in the inventory, and is added to all appropriate device groups.

## Key Considerations

The following section provides useful information and advice on the Device Window.

### Deleting Devices

A device deleted from one device group removes it from all device groups. The only way to re-add the device is to either re-import it or use the *Add Device* dialog.

### Active Selection

The active selection within 3Com Network Administrator is always highlighted in blue (this color may differ according to the windows scheme currently being used). A non-active selection is always shown in gray. The active selection may be contained within the device groups tree or the device list, but never both at the same time.

### Scheduled Tasks

When 3Com Network Administrator is closed all currently scheduled tasks are cancelled. When the application runs again the tasks will have to be re-scheduled.

# 4 Device Administration

## Overview

This chapter describes the following device administration functions:

- Web Management — launches your default web browser against a device selected in the device list.
- Telnet Management — launches your computer's Telnet application against a device selected in the device list.
- Administration Menu — contains integrated add-on 3Com device management applications.
- Registering Devices for Warranty — enables you to register the 3Com devices on your network for any applicable warranty.

The following topics are covered in this chapter:

- Key Concepts
- Components
- Examples
- Key Considerations

## Key Concepts

The following section describes the key concepts for administering devices using 3Com Network Administrator.

### Web Management

Many 3Com devices provide a web interface that enables you to manage a single device or stack of devices at one time. Your default web browser is used to display the web interface. Access to the interface is protected by username and password authentication. A graphical representation of the device is usually displayed, along with various device configuration options and low-level statistics. For more information on the features provided by the web interface, please refer to the user documentation for your device.

### Telnet Management

Most 3Com devices provide a Telnet management interface, enabling you to manage a single device or stack of devices at one time. Access to the interface is protected by username and password authentication. It typically provides the most complete range of configuration options. For more information on the features provided by the Telnet interface, please refer to the user documentation for your device.

### Administration Menu

The administration menu of 3Com Network Administrator contains entries for add-on 3Com device management applications. These applications provide management operations specific to a particular device type. For more information please refer to the appropriate management application’s manual and or online help pages.

ℹ *Devices that support the features described in the Administration Menu are listed in Appendix A on page 241.*

### 3Com Device View

Using Device View, along with the Device Configuration Tool, you can view and modify the configuration of a single device or multiple devices at the same time.

*For further information see Appendix B on page 251.*

*For information on devices supported by Device View, see Appendix A on page 241.*

### 3Com Switch Manager

Switch Manager is the element manager of the Switch 7700.

### 3Com Router Manager

Router Manager is the element manger of the 3Com router family.

### Network Jack Configuration Manager

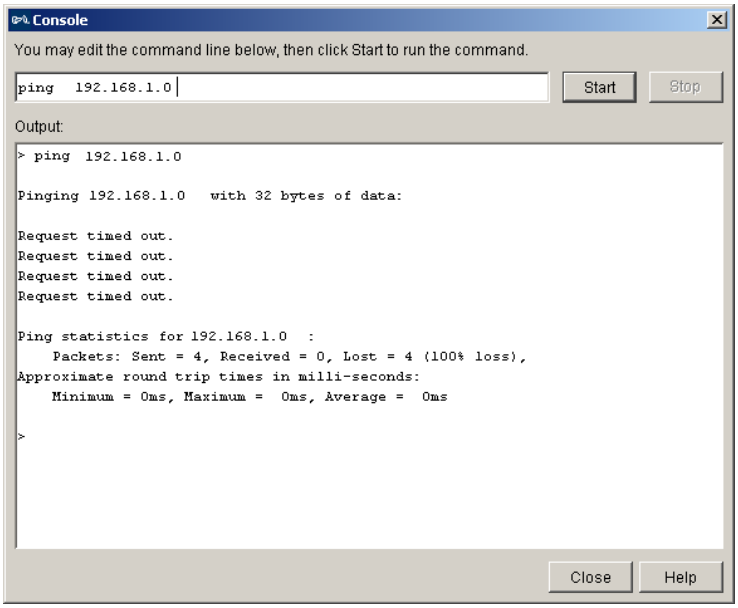
3Com Network Jack Configuration Manager provides management for the 3Com Network Jack NJ200. Although the NJ200 is bundled with a Local Configuration Manager and a Central Configuration Manager, only the Central Configuration Manager is integrated with 3Com Network Administrator. The Central Configuration Manager enables remote discovery, advanced configuration and management of multiple NJ200s.

## IP Ping

IP Ping enables you to run the Windows system ping command from within a command window. If you select a device that has more than one IP address, the IP ping menu will contain submenus for each IP address.

When you select a device and click on *IP Ping...* from the right-click menu, a console dialog is launched as shown in Figure 23:

**Figure 23** IP Ping Console Dialog



You may edit the command line below, then click Start to run the command.

```
ping  192.168.1.0
```

```
> ping  192.168.1.0

Pinging 192.168.1.0   with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.0   :
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

>
```

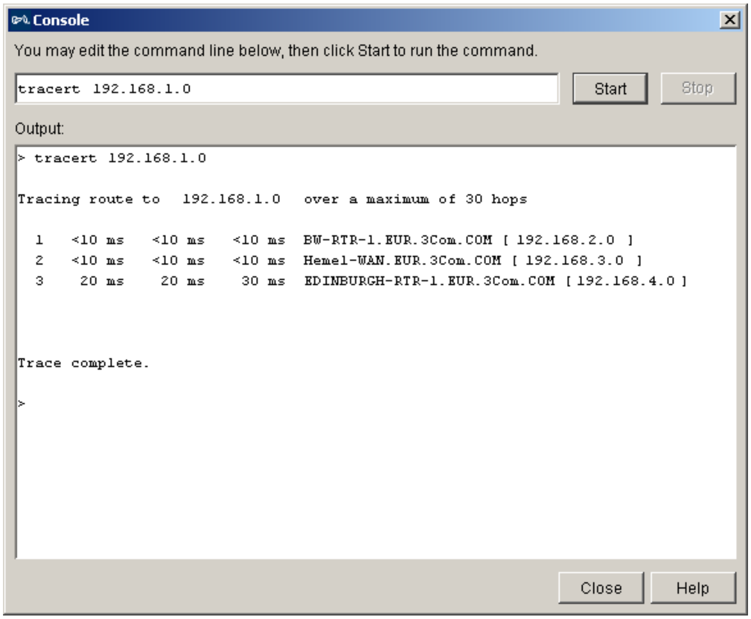
The dialog pre-fills the command line text box with the command 'ping' followed by the IP address of the device you have selected. The command line is provided so that you can specify additional command line options to the ping command. When you click *Start*, the ping command is run and its output is displayed in the *Output* window.

## Trace Route

The Trace Router feature enables you to run the Windows system 'tracert' utility. This utility lets you trace the router path from the management station to the device you're interested in. If the device has more than one IP interface, the Trace Route menu will contain submenus for each IP address the device has.

When you select a device and click on *Trace Route...* from the right-click menu, a console dialog is launched as shown in Figure 24:

**Figure 24** Trace Route Console Dialog



Console
You may edit the command line below, then click Start to run the command.
Start
Stop
Output:
Close
Help

```
tracert 192.168.1.0
```

```
> tracert 192.168.1.0

Tracing route to  192.168.1.0  over a maximum of 30 hops

  1   <10 ms   <10 ms   <10 ms  BW-RTR-1.EUR.3Com.COM [ 192.168.2.0 ]
  2   <10 ms   <10 ms   <10 ms  Hemel-WAN.EUR.3Com.COM [ 192.168.3.0 ]
  3    20 ms    20 ms    30 ms  EDINBURGH-RTR-1.EUR.3Com.COM [ 192.168.4.0 ]



Trace complete.

>
```

The dialog pre-fills the command line text box with the command ‘tracert’ and the IP address of the device you have selected. The command line is provided so that you can specify additional command line options to the trace route command. When you click *Start*, the trace route command is run and it’s output is displayed in the *Output* window.

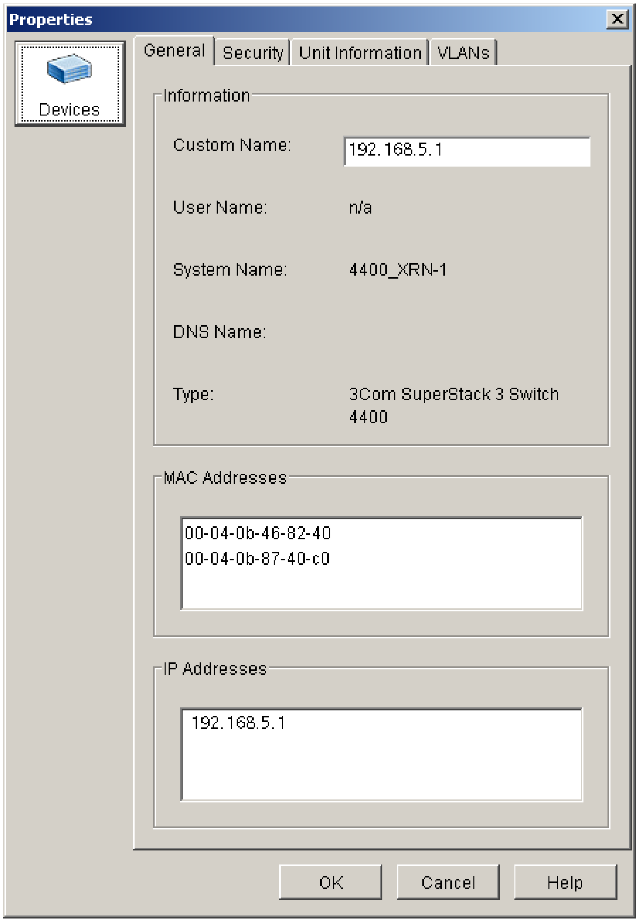
## Properties Dialog

The Device Properties dialog gives you additional details on a a selected device. The details are split in to four tabs as follows:

### General

The *General* tab provides name and address information for your device as shown in Figure 25. The name of the device and all MAC and IP addresses associated with it are displayed in this tab. You can change the name by editing the *Name* text field and clicking *OK*.

**Figure 25** Properties - General Tab



Information

Custom Name: 192.168.5.1

User Name: n/a

System Name: 4400_XRN-1

DNS Name:

Type: 3Com SuperStack 3 Switch 4400

MAC Addresses

00-04-0b-46-82-40
00-04-0b-87-40-c0

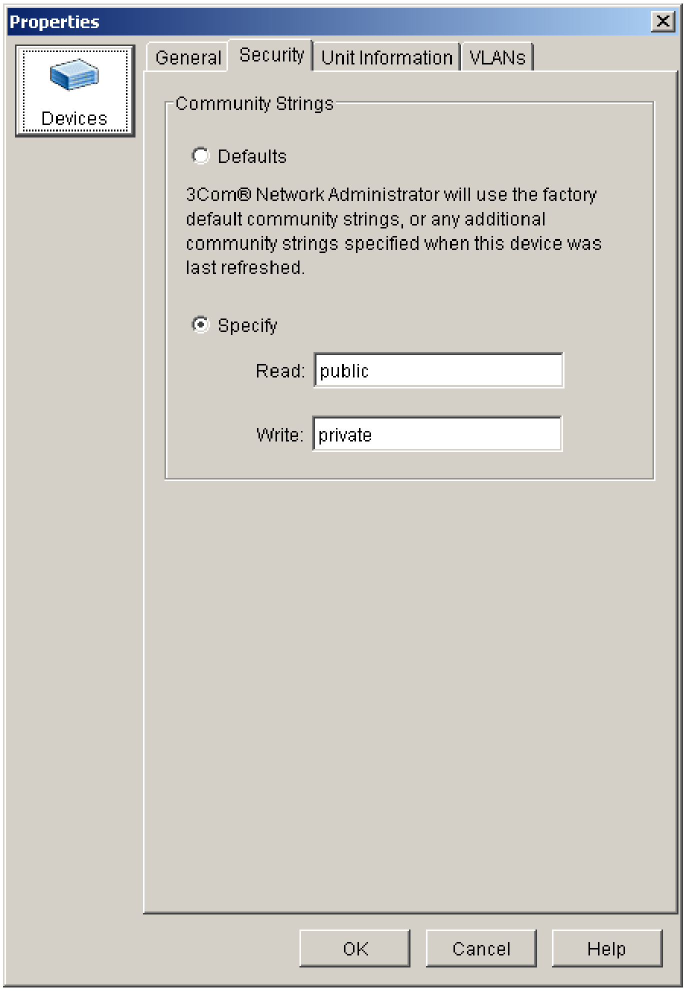
IP Addresses

192.168.5.1

## Security

The *Security* tab displays community string information as shown in Figure 26:

**Figure 26** Properties - Security Tab



Community Strings

○ Defaults

3Com® Network Administrator will use the factory default community strings, or any additional community strings specified when this device was last refreshed.

● Specify

Read: public

Write: private

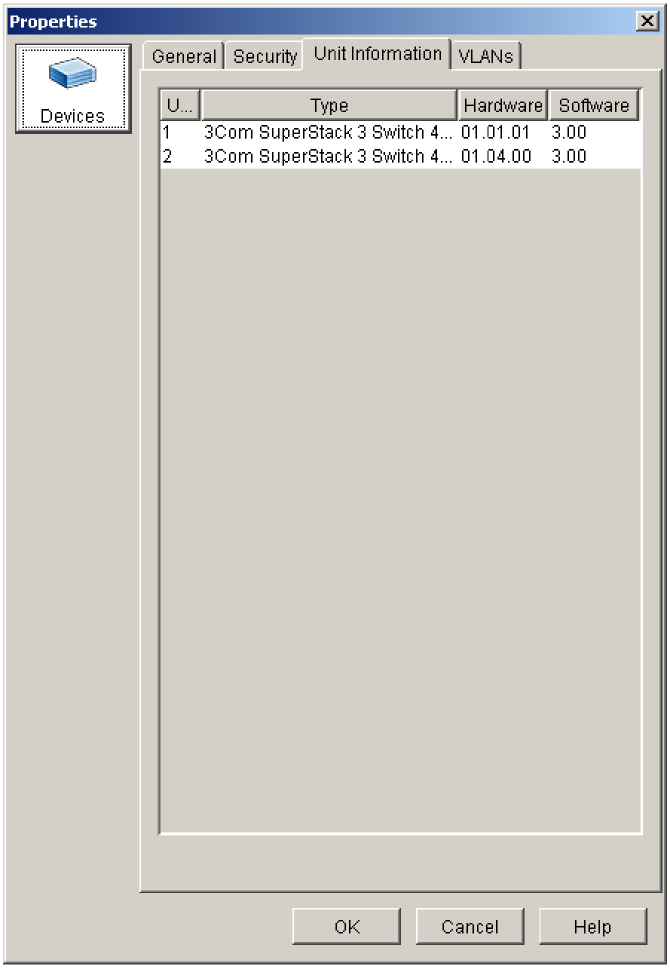
The following two radio buttons are provided:

- **Defaults** — select this option to use the community strings 3Com Network Administrator is using by default on all other devices. If this community string does not work, 3Com Network Administrator will resort to using the factory defaults for devices of that device type.
- **Specify** — select this option to specify the exact community strings to use for the selected device. You might use this option if you imported your devices using 'read-only' community strings but you now want to use the additional permissions that read-write access gives you.

### Unit Information

The *Unit Information* tab lists the various units in a stack. The individual device types, with hardware and software revision are shown in the table in Figure 27:

**Figure 27** Properties - Unit Information Tab



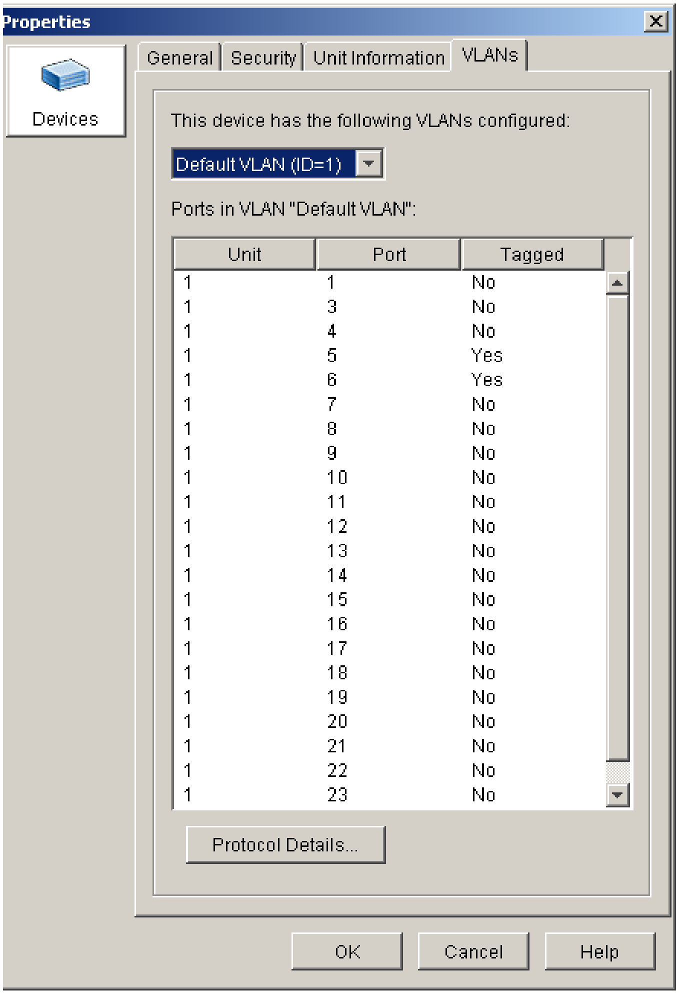
| U... | Type | Hardware | Software |
|---|---|---|---|
| 1 | 3Com SuperStack 3 Switch 4... | 01.01.01 | 3.00 |
| 2 | 3Com SuperStack 3 Switch 4... | 01.04.00 | 3.00 |

You can resize the columns in the unit information table by dragging the edges of the table headings. You can also change the order of the columns by dragging the column headings.

## VLANs

The *VLANs* tab contains detailed VLAN information for the selected device as shown in Figure 28:

**Figure 28** Properties - VLANs Tab



This device has the following VLANs configured:

Default VLAN (ID=1)

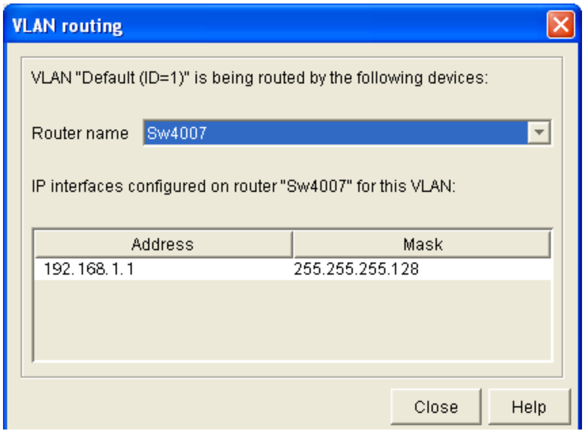
Ports in VLAN "Default VLAN":

| Unit | Port | Tagged |
|---|---|---|
| 1 | 1 | No |
| 1 | 3 | No |
| 1 | 4 | No |
| 1 | 5 | Yes |
| 1 | 6 | Yes |
| 1 | 7 | No |
| 1 | 8 | No |
| 1 | 9 | No |
| 1 | 10 | No |
| 1 | 11 | No |
| 1 | 12 | No |
| 1 | 13 | No |
| 1 | 14 | No |
| 1 | 15 | No |
| 1 | 16 | No |
| 1 | 17 | No |
| 1 | 18 | No |
| 1 | 19 | No |
| 1 | 20 | No |
| 1 | 21 | No |
| 1 | 22 | No |
| 1 | 23 | No |

Clicking on the drop-down list will list all VLANs associated with the device. Each time you select a VLAN, the table under the drop-down list changes to show the ports that are members of that VLAN.

If a VLAN is being used for routing, click *VLAN Routing* to launch a separate dialog listing the subnets and routers that use that VLAN for routing as shown in Figure 29:

**Figure 29** Properties - VLANs Tab - VLAN Routing



VLAN routing

VLAN "Default (ID=1)" is being routed by the following devices:

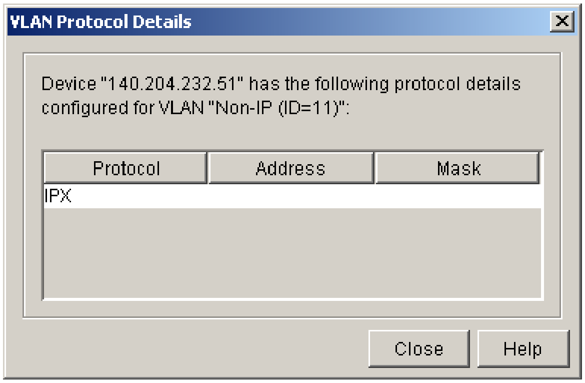
Router name: Sw4007

IP interfaces configured on router "Sw4007" for this VLAN:

| Address | Mask |
|---|---|
| 192.168.1.1 | 255.255.255.128 |

If a VLAN is being used to constrain certain protocols the *Protocol Details* button is available. Click *Protocol Details* to launch a dialog that lists the network protocols that are associated with the VLAN as shown in Figure 30:

**Figure 30** Properties - VLANs Tab - VLAN Protocol Details



VLAN Protocol Details

Device "140.204.232.51" has the following protocol details configured for VLAN "Non-IP (ID=11)":

| Protocol | Address | Mask |
|---|---|---|
| IPX | | |

### Registering Devices for Warranty

You can register the 3Com devices on your network for any applicable warranty. 3Com Network Administrator checks for devices on your network that have not yet been registered and sends this information to 3Com. See "What Data is Sent to the 3Com server" on page 78 for more details.

*Registering devices enables the device warranty for all the supported 3Com equipment and enables 3Com services such as technical assistance, hardware repair and hardware replacement.*

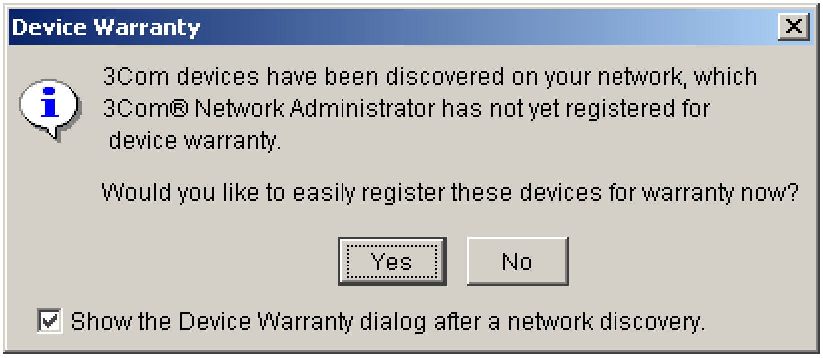
## Components

The following sections describe how to administer devices using 3Com Network Administrator.

### Device Warranty Dialog

When a refresh operation completes and 3Com Network Administrator finds that there are unregistered devices, you are given the option to register devices as shown in Figure 31:

**Figure 31** Device Warranty Dialog



Device Warranty

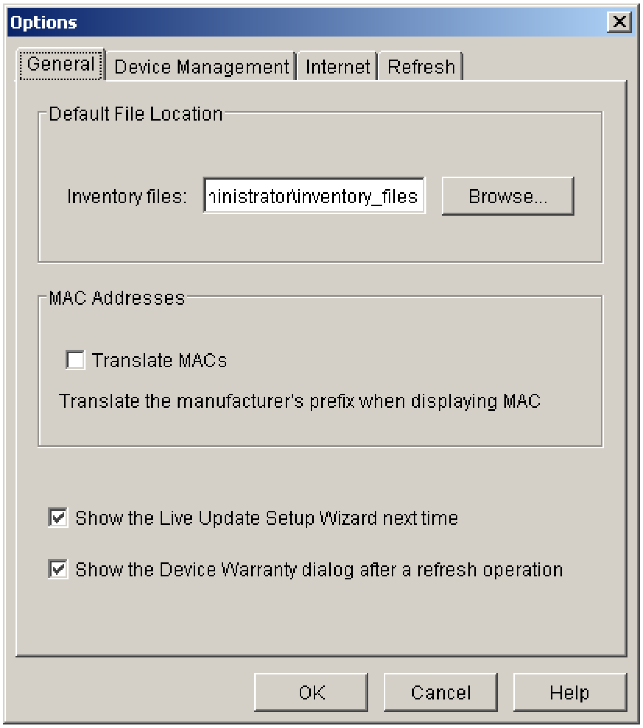
3Com devices have been discovered on your network, which 3Com® Network Administrator has not yet registered for device warranty.

Would you like to easily register these devices for warranty now?

☑ Show the Device Warranty dialog after a network discovery.

If you do not want to see this dialog after each refresh, de-select the *Show the Device Warranty dialog after a network discovery* check box. You can also de-select the *Show the Device Warranty dialog after a refresh operations* check box in the *General* panel of the *Options* dialog as shown in Figure 32.

**Figure 32** Options - General



Inventory files: ninistrator\inventory_files

□ Translate MACs

Translate the manufacturer's prefix when displaying MAC

☑ Show the Live Update Setup Wizard next time

☑ Show the Device Warranty dialog after a refresh operation

## Device Warranty Wizard

The Device Warranty wizard allows you to enter registration information and to select the devices you want to register for any applicable warranty.

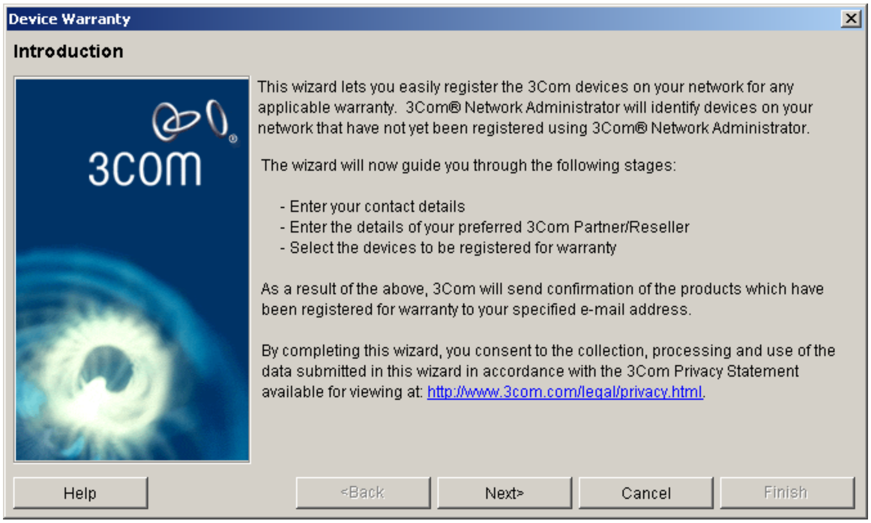
To launch the wizard:

- Click *Yes* from the *Device Warranty* dialog, as shown in Figure 31. Or,
- Select the *Tools* > *Device Warranty* menu option

### Introduction Step

The *Introduction* step describes the various stages of the wizard and provides a hyperlink to the 3Com Privacy Statement as shown in Figure 33.

**Figure 33** Introduction Step



**Introduction**

This wizard lets you easily register the 3Com devices on your network for any applicable warranty. 3Com® Network Administrator will identify devices on your network that have not yet been registered using 3Com® Network Administrator.

The wizard will now guide you through the following stages:

- Enter your contact details
- Enter the details of your preferred 3Com Partner/Reseller
- Select the devices to be registered for warranty

As a result of the above, 3Com will send confirmation of the products which have been registered for warranty to your specified e-mail address.

By completing this wizard, you consent to the collection, processing and use of the data submitted in this wizard in accordance with the 3Com Privacy Statement available for viewing at: http://www.3com.com/legal/privacy.html.

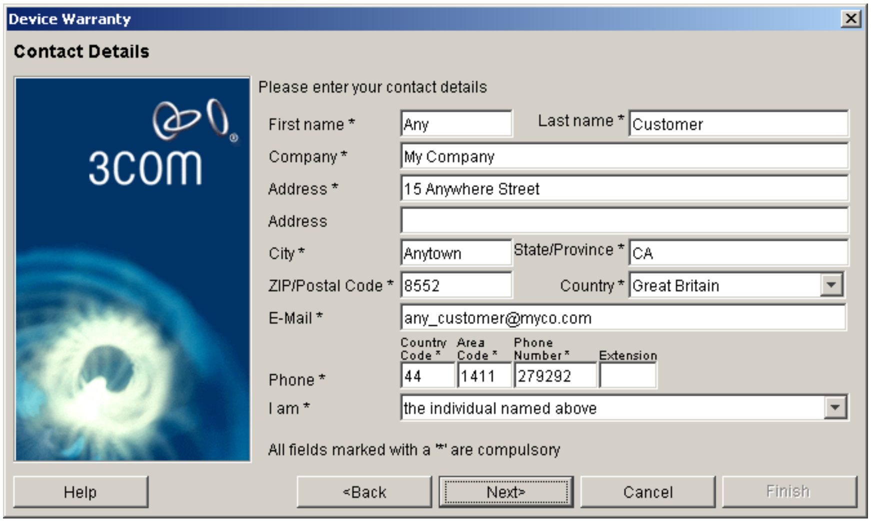
Click on the hyperlink to view the 3Com Privacy Statement in your default web browser.

*By clicking* Next, *you consent to the collection, processing and use of the data submitted in the Device Warranty Wizard, in accordance with the 3Com Privacy Statement.*

## Contact Details Step

The *Contact Details* step allows you to enter your contact information as shown in Figure 34.

**Figure 34** Contact Details Step



Device Warranty

**Contact Details**

Please enter your contact details

First name * Any

Last name * Customer

Company * My Company

Address * 15 Anywhere Street

Address

City * Anytown

State/Province * CA

ZIP/Postal Code * 8552

Country * Great Britain

E-Mail * any_customer@myco.com

Phone * Country Code * 44 Area Code * 1411 Phone Number * 279292 Extension

I am * the individual named above

All fields marked with a '*' are compulsory

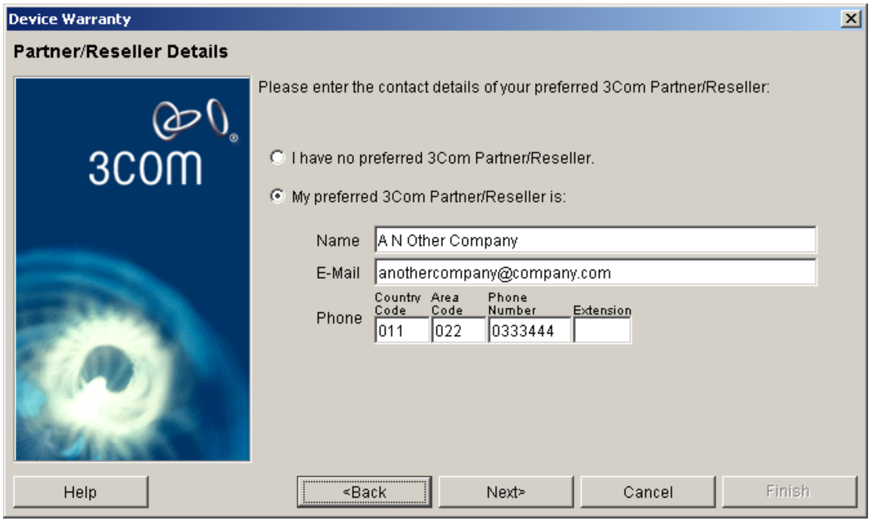
All fields are compulsory (marked with a '*'), except the second line of the Address and the Phone Extension number

*3Com Network Administrator retains these details for the next time you run the Device Warranty Wizard. This way, you only have to enter your contact details once.*

### Partner/Reseller Details Step

The *Partner/Reseller Details* step enables you to enter contact details for your preferred 3Com Partner/Reseller as shown in Figure 35.

**Figure 35** Partner/Reseller Details Step



Device Warranty

Partner/Reseller Details

Please enter the contact details of your preferred 3Com Partner/Reseller:

○ I have no preferred 3Com Partner/Reseller.

● My preferred 3Com Partner/Reseller is:

Name: A N Other Company

E-Mail: anothercompany@company.com

| | Country Code | Area Code | Phone Number | Extension |
|---|---|---|---|---|
| Phone | 011 | 022 | 0333444 | |

The *Partner/Reseller Details* step displays the following fields:

- **I have no preferred 3Com Partner/Reseller** — select this option if you do not order 3Com equipment from an approved 3Com Partner/Reseller.
- **My preferred 3Com Partner/Reseller is** — select this option if you order 3Com equipment from an approved 3Com Partner/Reseller.

These fields are only displayed if you select the *My preferred 3Com Partner/Reseller is* option:

- **Name** — the company name of your preferred 3Com Partner/Reseller.
- **E-Mail** — the contact e-mail for your preferred 3Com Partner/Reseller.
- **Phone** — the contact phone number for your preferred 3Com Partner/Reseller.

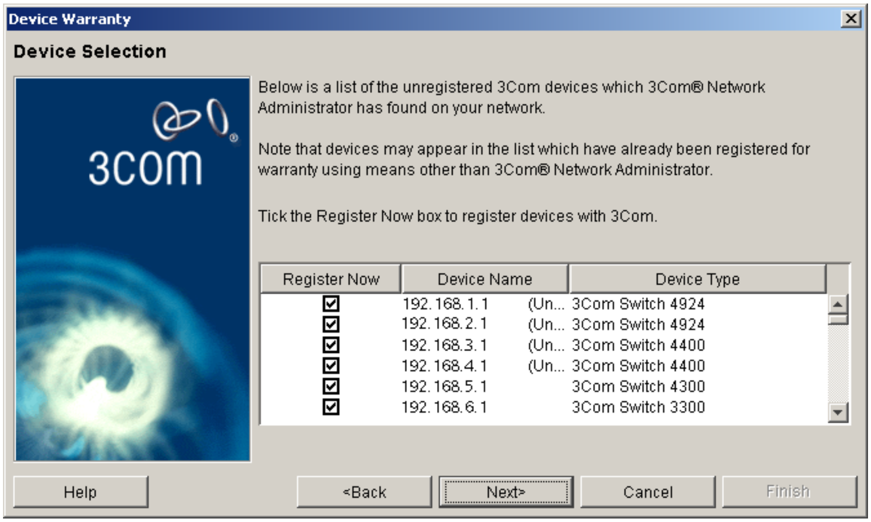
*If you select the* My preferred 3Com Partner/Reseller is *option, the* Name *field cannot be left blank.*

Just like your contact details, 3Com Network Administrator retains the reseller details for the next time you run the Device Warranty Wizard. This way, you only have to enter your reseller's contact details once.

## Device Selection Step

The *Device Selection* step lists the 3Com devices on your network that have not yet been registered as shown in Figure 36.

**Figure 36** Device Selection Step



Device Warranty

Device Selection

Below is a list of the unregistered 3Com devices which 3Com® Network Administrator has found on your network.

Note that devices may appear in the list which have already been registered for warranty using means other than 3Com® Network Administrator.

Tick the Register Now box to register devices with 3Com.

| Register Now | Device Name | Device Type |
|---|---|---|
| ☑ | 192.168.1.1 (Un... | 3Com Switch 4924 |
| ☑ | 192.168.2.1 (Un... | 3Com Switch 4924 |
| ☑ | 192.168.3.1 (Un... | 3Com Switch 4400 |
| ☑ | 192.168.4.1 (Un... | 3Com Switch 4400 |
| ☑ | 192.168.5.1 | 3Com Switch 4300 |
| ☑ | 192.168.6.1 | 3Com Switch 3300 |

Each row in the list corresponds to a 3Com product. If the device in the inventory file is a stack, the list will contain one row per unit. If the network node in the inventory is a chassis device, the list will contain one row for each chassis blade.

The *Device Selection* step contains the following columns:

- **Register Now** — when the check box in this column is selected, the corresponding device will be registered for warranty. De-select the check box if you do not want this device to be registered
- **Device Name —** the name of the device as it appears in the inventory file. If the row corresponds to a unit (for a stack) or a blade (for a chassis), the index of the unit or blade will also be specified. For instance, *MySwitch (Unit 2)*.
- **Device Type** — the type of the product.

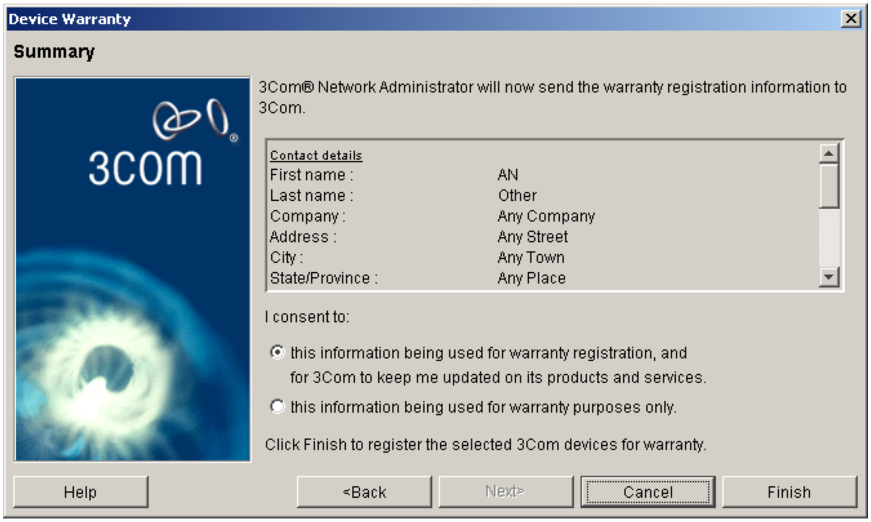
*By default, all supported 3Com devices are listed and selected.*

*If you de-select some devices and complete the wizard, the next time you run the Device Warranty wizard, these devices will be listed and de-selected by default.*

### Summary Step

At the *Summary* step you can review the contact details you specified in the previous steps of the wizard as shown in Figure 37.

**Figure 37** Summary Step



Device Warranty

Summary

3Com® Network Administrator will now send the warranty registration information to 3Com.

Contact details

| | |
|---|---|
| First name : | AN |
| Last name : | Other |
| Company : | Any Company |
| Address : | Any Street |
| City : | Any Town |
| State/Province : | Any Place |

I consent to:

● this information being used for warranty registration, and for 3Com to keep me updated on its products and services.

○ this information being used for warranty purposes only.

Click Finish to register the selected 3Com devices for warranty.

The *Summary* step provides a summary of the warranty registration information prior to sending it to 3Com. If you consent to 3Com keeping you updated on its products you will receive 3Com product news.

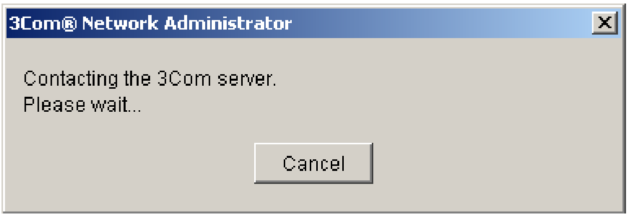
*If you selected* I am registering on behalf of the individual named above *in the* Contact Details *step of the wizard, then the first* I consent to: *option will be greyed out.*

Click *Finish* to connect to the 3Com server and register the devices for warranty.

## Connection to the 3Com Server

While 3Com Network Administrator is connecting to the 3Com server, a message, as shown in Figure 38, is displayed:

**Figure 38** Connecting to the 3Com Server



3Com® Network Administrator

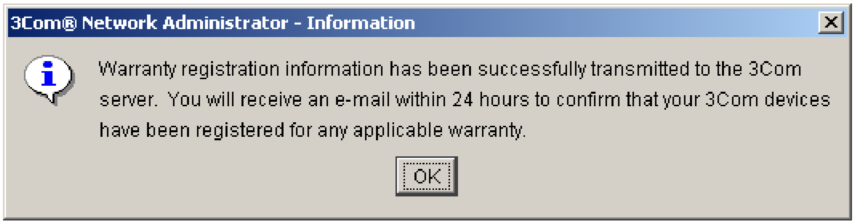
Contacting the 3Com server.
Please wait...

Click *Cancel* if you wish to interrupt the connection and abort the registration of your 3Com devices.

Once 3Com Network Administrator is connected to the 3Com server, the data will be transmitted and the message will update.

Once the transmission is complete, a confirmation message is displayed as shown in Figure 39.

**Figure 39** Confirmation Message



3Com® Network Administrator - Information

Warranty registration information has been successfully transmitted to the 3Com server. You will receive an e-mail within 24 hours to confirm that your 3Com devices have been registered for any applicable warranty.

3Com will send you an email within 24 hours to confirm that your 3Com devices are now registered for any applicable warranty.

## What Data is Sent to the 3Com server

To register your 3Com devices, 3Com Network Administrator will transmit some data to the 3Com server. That data consists of:

- The contact details (name, company, address etc) that you specified in the Device Warranty wizard.
- The contact details of your preferred 3Com Partner/Reseller (name, email etc) that you specified in the Device Warranty wizard (if any).
- The details of the device you want to register (product number, serial number, MAC address).

*For security reasons, 3Com Network Administrator does not send the IP address of your devices.*

This information is then processed so that the devices are registered for their applicable warranty.

## Reports

The following reports are produced when administering devices.

### Web Management

Devices that support the web interface can be listed by generating a custom report as follows:

1. From 3Com Network Administrator, launch the *Reports* dialog from *Tools* > *Reports.*
2. Click *Custom Report Types*.
3. Click *Add* from the *Custom Report Types* dialog to launch the Add Report Type wizard.
4. In the first step of the wizard, include the *Web management* column in the report to be generated. Click *Next.*
5. In the second step of the wizard, give the report a name and (optionally) a description. Click *Finish*.
6. Click *OK* to close the *Custom Report Types* dialog.
7. Run the custom report by clicking on its name in the *Report Types* column of the *Reports* dialog and clicking *Generate Reports*.

### Device Warranty

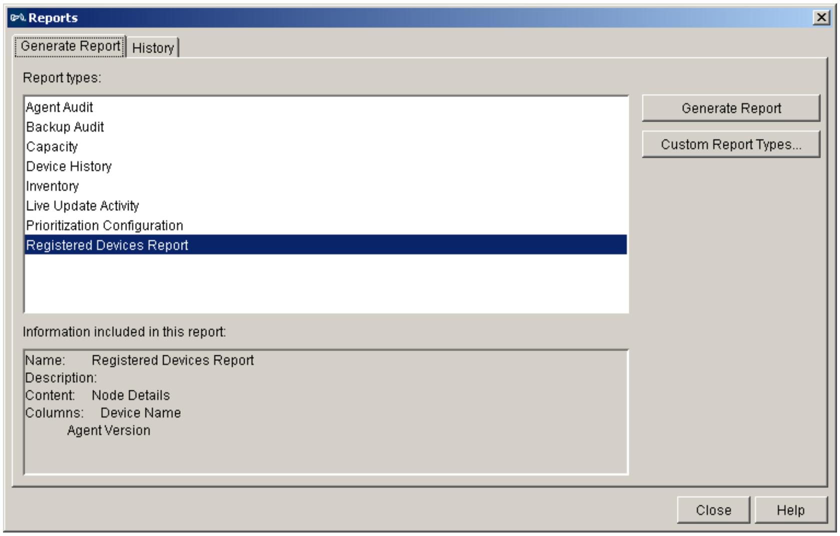
You can generate a report on the devices on your network that 3Com Network Administrator registered for any applicable warranty as follows:

1. From 3Com Network Administrator, launch the *Reports* dialog from *Tools* > *Reports*.
2. Click *Custom Report Types*.
3. Click *Add* from the *Custom Report Types* dialog to launch the Add Report Type wizard.
4. In the first step of the wizard, include the *Registered* column in the report, as well as columns that help you identify the device (for instance, *Device Name*, *Product Number*, *Serial Number*). Click *Next.*
5. In the second step of the wizard, give the report a name and (optionally) a description. Click *Next* to show the *Summary* dialog and click *Finish*.

**6** Click *OK* to close the *Custom Report Types* dialog.

**7** In the *Report Types* table, click the name of the report you created and click on *Generate Report* to launch the report as shown in Figure 40.

**Figure 40** Device Warranty



Report types:

- Agent Audit
- Backup Audit
- Capacity
- Device History
- Inventory
- Live Update Activity
- Prioritization Configuration
- Registered Devices Report

Information included in this report:

Name: Registered Devices Report
Description:
Content: Node Details
Columns: Device Name
Agent Version

When you view the report you have generated the *Registered* column shows:

- **Yes** — if 3Com Network Administrator registered the product.
- **No** — if 3Com Network Administrator did not register the product.
- **N/A** — if the product is not supported by the Device Warranty feature.

## Examples

The following section provides some examples of how to administer the devices on your network.

### Renaming a Switch 4007 using Telnet

You have a Switch 4007 on your network and you wish to rename it using the Telnet Management Interface. To do this:

1. Find the Switch 4007 device in the 3Com Network Administrator device list. This can be done using *Edit* > *Find* if needed.
2. Select the device and right-click on it to launch the right-click menu.
3. Select the *Telnet Management* menu item. The Telnet console will be launched.
4. Enter your username and password for the device.
5. Type *set name < new name >.*
6. Type *logout.* The Telnet console will close.
7. Use *Refresh* to update the current inventory file with the new name.

### Disabling a Port on a Switch 4400 using the Web Interface

You have a Switch 4400 on your network and you wish to disable a port on it using the web interface:

1. Find the appropriate Switch 4400 device in the 3Com Network Administrator device list. This can be done using the *Find* dialog if needed.
2. Select the device and right-click on it to launch the right-click menu.
3. Select the *Web Management* menu item. The default web browser will be launched.
4. Enter your username and password for the device.
5. Select the *Device View* tab in the web browser.
6. Right-click on the port and select *Setup.*
7. Change the Port State to *Disabled* and click *OK*.
8. Close the web browser.

## Viewing Connected Ports using Device View

You have a Switch 3300 on your network and you wish to view connected ports on it using Device View:

1. Find the appropriate Switch 3300 device in the 3Com Network Administrator device list. This can be done using the *Find* dialog if needed.
2. Select the device and right-click on it to launch the menu.
3. Select *Device > Administration > Device View.*

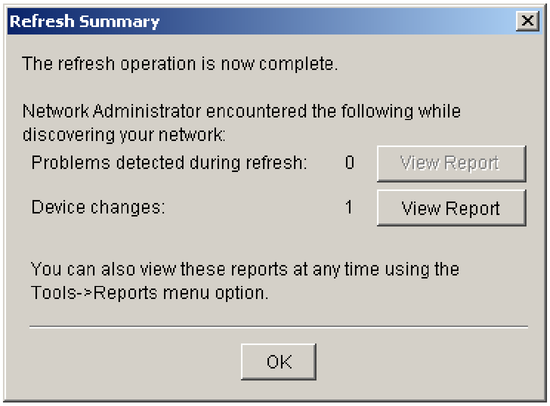
   Device View will be launched and a graphical representation of the device will be displayed. Connected ports have a connected link annotation over them. If the port is 'up' it will be green in color.

## Registering 3Com Devices for Warranty

You have just bought several 3Com devices and installed them on your network. You now want to register all these devices for warranty using 3Com Network Administrator.

1. Launch the *Options* dialog using *Tools > Options* and make sure that in the *General* tab, the *Show the Device Warranty dialog after a refresh operation* option is selected. If it is de-selected, click on the check box to select it.
2. Re-import the network on which the new 3Com devices are installed. This can be done by launching the right-click menu and selecting *Refresh Information*.
3. When the refresh is complete, you will get a message as shown in Figure 41.

**Figure 41** Registering Devices for Warranty - Example



The refresh operation is now complete.

Network Administrator encountered the following while discovering your network:

Problems detected during refresh: 0

Device changes: 1

You can also view these reports at any time using the Tools->Reports menu option.

**4** Click *OK* to launch the Device Warranty wizard.

**5** In the *Introduction* step, make sure you have read the 3Com Privacy Statement and click *Next.*

**6** In the *Contact Details* step ensure:

- If this is the first time you have used the wizard, that you enter your contact details and click *Next*. Alternatively,
- If you have previously completed the wizard, you review the contact details as they will be pre-set and click *Next.*

**7** In the *Reseller Details* step ensure:

- If this is the first time you have used the wizard, enter the contact details of your preferred 3Com Partner/Reseller (if any). Alternatively,
- If you have previously completed the wizard, the contact details of your preferred 3Com Partner/Reseller (if any) will be pre-set so review the details and click *Next*.

**8** In the *Device Selection* step, make sure that your new devices are included and that the *Register Now* check box is selected for those devices. Click *Next*.

**9** In the *Summary* step, make sure that the contact details are correct and click *Finish*.

The registration details will be communicated to the 3Com server and a message box will be displayed to confirm the completion of the operation.

You will also get a confirmation by email that the devices you selected have been registered by 3Com for any applicable warranty.

## Key Considerations

The following section provides assistance when administering devices.

### Troubleshooting

Some advice on errors are outlined as follows:

**The Device Warranty dialog is not displayed after a refresh**

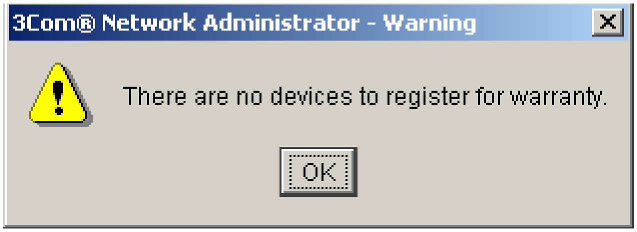
One possible explanations for this is that the *Device Warranty* dialog is disabled. To check this:

1. Launch the *Options* dialog by selecting the *Tools* > *Options* menu.
2. Select the *General* tab.
3. Check that the *Show the Device Warranty dialog after a refresh operation* check box is selected. If it is not selected, click on the check box to select this option.

The other explanation for this is that there are no devices to register. To check this:

1. Select the *Tools* > *Device Warranty* menu option.
2. If all the devices on your network have already been registered, a message, as shown in Figure 42, is displayed.

**Figure 42** Warning Message



3Com® Network Administrator - Warning

There are no devices to register for warranty.

**3Com Network Administrator lists some devices as unregistered, although you have already registered them on the 3Com website**

The reason for this is that 3Com Network Administrator only knows about devices that were registered using 3Com Network Administrator. If the devices were registered on the 3Com website, 3Com Network Administrator will think these devices are as yet unregistered.

If you do register these devices again, this will not affect the original registration.

## Frequently Asked Questions

Below are some frequently asked questions about the device warranty confirmation email.

### Why are some registered devices missing from the email?

If the device selection includes devices that have already been registered (for instance, if you registered them on the 3Com website), these devices will not be listed in the confirmation email.

### Why is there no warranty associated with some of the devices in the email?

There are two explanations for this:

- The product is not supported by 3Com anymore — if the product has been discontinued, there will be no warranty for that product.
- The warranty date has expired — if the warranty period for a device has expired, there will be no warranty for that device.

# 5 IMPORTING AND REFRESHING DEVICES

## Overview

This chapter describes how to populate the inventory with a list of devices so that they appear in the device list. You must do this before you can perform administrative operations on your devices, such as agent update and device backup.

The process of populating the inventory is done in two stages as follows:

- **Importing** — enables you to supply 3Com Network Administrator with an initial list of devices from an external source. 3Com Network Administrator supports two data sources for importing:
  - A text file of devices in Comma Separated Value (CSV) format.
  - A populated HP OpenView database
- **Refreshing** — begins once you have imported a list of devices. 3Com Network Administrator attempts to 'interrogate' each imported device in order to obtain live information about its detailed configuration. A device will only be added to the inventory if the information obtained meets certain criteria (for example, only 3Com devices are supported). You can also use the refresh operation independently to keep your inventory up-to-date.

The following topics are covered in this chapter:

## Key Concepts

This section outlines the key concepts of importing and refreshing.

### Importing

3Com Network Administrator provides two methods for importing devices from an external source into its inventory. It enables you to import a list of devices from a text file or, alternatively, from HP OpenView. After importing a list of devices, 3Com Network Administrator performs a refresh operation to obtain live information from the devices.

#### Importing from HP OpenView

Device data retrieved by HP OpenView is stored in a database. You can import some or all 3Com devices from the HP OpenView database into 3Com Network Administrator's own inventory. This allows you to use the administrative tools provided by 3Com Network Administrator to manage 3Com devices.

Typically, if you have a large network or if your network is spread across multiple sites then it is likely that it will be divided into subnets. When HP OpenView retrieves information about your network, it detects which subnet(s) a device belongs to. 3Com Network Administrator makes use of this information when importing from HP OpenView and allows you to choose which subnets you wish to import device information from. This can speed up the import process as it eliminates unnecessary processing of devices from subnets that you are not interested in.

*If you find that this importing process does not provide the level of control you require for customizing your inventory, you can delete unwanted devices from the inventory once the import process is complete. Alternatively, you can use the CSV file import mechanism or simply add single devices one at a time using the 'Add Device' feature.*

*Since the management tools that 3Com Network Administrator provides are specific to 3Com devices, it only imports 3Com devices from HP OpenView. If a device does not appear as a 3Com device in the HP OpenView database, it will not be imported.*

### Importing from CSV Files

CSV files are simple text files used to specify a set of data. The data is made up of a number of records, with each record corresponding to a line in the file. Each record is made up of a number of fields, where each field is separated by a comma.

You can create a CSV file to specify the list of devices that you wish to import into the 3Com Network Administrator inventory. Each record (or line) corresponds to the device that you wish to import. The fields within a record correspond to parameters associated with the device, such as a name or IP address. The format of a device record expected by 3Com Network Administrator is:

```
IP address,[subnet mask],[name],[read community],[write
community]
```

The purpose of each field is as follows:

- **IP Address** — the address used by the refresh operation to communicate with the device. Only the IP address is mandatory.
- **Subnet Mask** — used for grouping devices during the refresh operation. The subnets created in the inventory file may be different to those provided by the CSV file if a different subnet mask is read from the device.
- **Name** — defines the name of the device that will ultimately appear in the device list. If you do not provide a name here then 3Com Network Administrator will choose a name based on the information read from the device during the refresh operation.
- **Read Community** — the SNMP read community string that the refresh operation uses when reading detailed configuration information from the device, such as unit and port configuration. If you do not supply a read community, 3Com Network Administrator will default to using ‘public’.
- **Write Community** — required by 3Com Network Administrator for certain administration functions, such as traffic prioritization. The refresh operation attempts to verify that the write community you have provided is correct. If you do not supply write community then 3Com Network Administrator will attempt to use the factory default for that device.

### CSV File Format

3Com Network Administrator expects the content of the CSV file to obey certain rules as follows:

- Each record (device) should be on a separate line.
- White space at the start and end of a field is ignored.
- If an optional field is omitted within the middle of a line, the commas surrounding it must be present. For example, omitting the *name* field:

  ```
  192.168.1.2, 255.255.255.0,, public, private
  ```

- If an optional field is omitted at the end of a line, its preceding comma need not be present. For example, omitting the write community:

  ```
  192.168.1.2, 255.255.255.0., My Device, public
  ```

- Fields containing commas must be surrounded by double quotes. For example:

  ```
  192.168.1.2, 255.255.255.0., “Device, A”, public, private
  ```

- Blank lines are ignored and are not considered to be errors.
- Comment lines can be included and must be preceded by a “#” symbol. As with blank lines, they are ignored. For example:

  ```
  # This is the main router
  192.168.1.1, 255.255.255.0., Router A
  ```

*You can specify IP address ranges.*

## Refreshing

3Com Network Administrator ‘refreshes’ the device information by reading the live data from the devices on the network. 3Com Network Administrator refreshes the devices it intends to add to the inventory file and ultimately display in the device list.

3Com Network Administrator refreshes the devices it intends to add to the inventory file and ultimately display in the device list. 3Com Network Administrator ‘refreshes’ the device information by reading the live data from the devices on the network.

Many of the tools provided by 3Com Network Administrator require detailed knowledge of the configuration of the devices they are operating on. For example, Device Setup enables you to copy the software configuration of one 3Com device to another device of the same type. To be able to establish which devices are compatible for such an operation, 3Com Network Administrator needs to know their detailed hardware configuration. This is the information that the refresh operation retrieves for each device in the inventory file.

### Information Retrieved by Refresh

The refresh operation retrieves detailed information about a device, some of which is required by other tools within 3Com Network Administrator. This includes:

- Pinging the device to verify that the device still exists on the network.
- Reading the basic SNMP information of the device, such as its MAC address, name and location.
- Determining any services it supports, such as Telnet and Web management.
- Establishing the detailed hardware and software configuration of the device, such as unit and port information and the agent software version it is running, by using SNMP.

### Performing Refresh

3Com Network Administrator performs a refresh at the following times:

- **After an Import** — a refresh operation is always initiated automatically on a list of devices that were successfully imported from a CSV file or HP OpenView.
- **As a Manual Operation** — you can request a refresh on some or all devices in the current inventory. This is done by selecting the relevant devices and then selecting *Device > Refresh Information*. You may wish to do this if you have re-configured some of your devices. For example, if you have added a new unit to a stack.
- **As a Scheduled Operation** — you can run an automated refresh operation at periodic intervals by setting the frequency from the Refresh tab of the *Options* dialog.

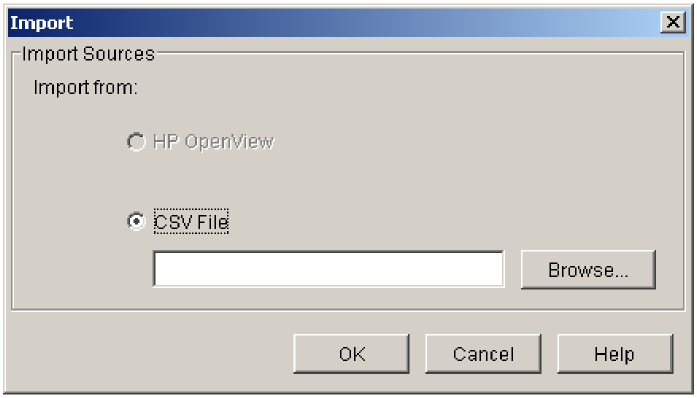
## Components

The following section describes how to import and refresh device information using 3Com Network Administrator.

### Import Dialog

The *Import* dialog can be launched from the *File* > *Import* menu as shown in Figure 43:

**Figure 43** Import Dialog



The *Import* dialog enables you to choose one of two data sources to import a list of devices from, as follows:

- **Import from HP OpenView** — to import devices using this option, HP OpenView must be installed.
- **Import from CSV File** — to import devices using this option you can manually enter a full path and filename into the *Edit* field or use *Browse* to search for the file on your computer.

### Import Progress Dialog

The *Import Progress* dialog displays when you select *OK* in the *Import* dialog and indicates how much of the import process is complete. When you are importing from HP OpenView a count is given of the number of devices processed. When you are importing from a CSV file a count is given of the number of lines processed. Click *Cancel* to stop the import operation at any time during this period.

When the import process is complete an Import report is generated containing a list of successfully imported devices and any problems encountered during the import process. The *Cancel* button is grayed out while the report is being generated.

*The report cannot be viewed at this point. It can only be viewed when the* Summary *dialog is displayed after the refresh operation has completed.*

The *Import Progress* dialog will eventually close automatically and the process continues one of two ways, as follows:

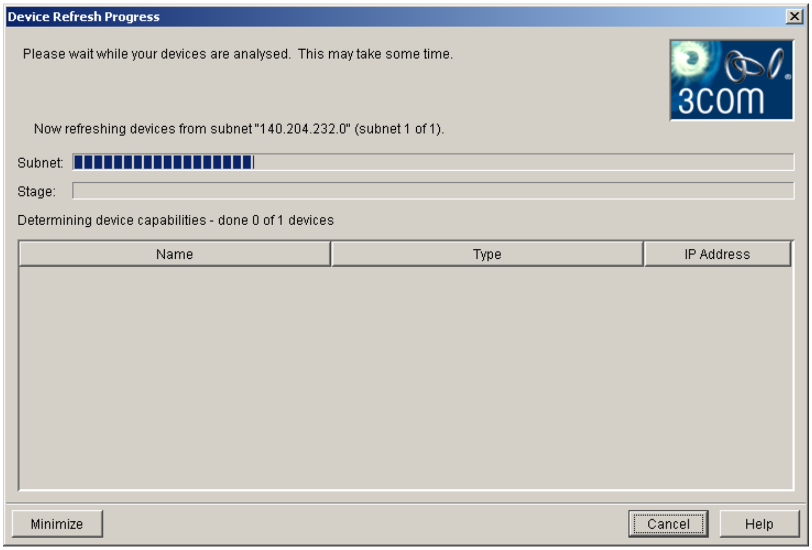
- If at least one device was successfully imported 3Com Network Administrator proceeds to the refresh operation in order to obtain live data for those devices.
- If no devices were successfully imported, the refresh operation is not performed. Instead, the *Summary* dialog is displayed allowing you to view the report in order to establish errors that may have occurred.

## Refresh Progress Dialog

The *Refresh Progress* dialog displays when a refresh operation starts and is shown for the duration of the refresh operation. It exists in two forms:

- **Restored** — this is the normal form as shown in Figure 44. It appears as a dialog showing a progress bar for the current subnet being processed and a progress bar for the current stage being processed within the subnet. As devices are processed successfully, they are added to the list box in the center of the dialog. The dialog can be cancelled or minimized at any time.

**Figure 44** Refresh Progress Dialog



Device Refresh Progress

Please wait while your devices are analysed. This may take some time.

Now refreshing devices from subnet "140.204.232.0" (subnet 1 of 1).

Subnet:

Stage:

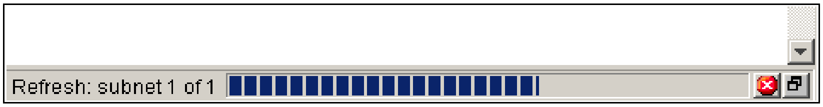
Determining device capabilities - done 0 of 1 devices

| Name | Type | IP Address |
|---|---|---|

- **Minimized** — the dialog itself is not visible but the progress bar is shown on the right hand part of the status bar. There are buttons to the right to cancel the refresh operation or restore the dialog to its visible state. You can minimize the *Refresh Progress* dialog by clicking *Minimize* in the bottom left hand corner of the dialog.

  If *Minimize* is selected, then the Minimize buttons are shown in the bottom right hand corner of the *Device Window* dialog as shown in Figure 45:

**Figure 45** Minimized Buttons



Refresh: subnet 1 of 1

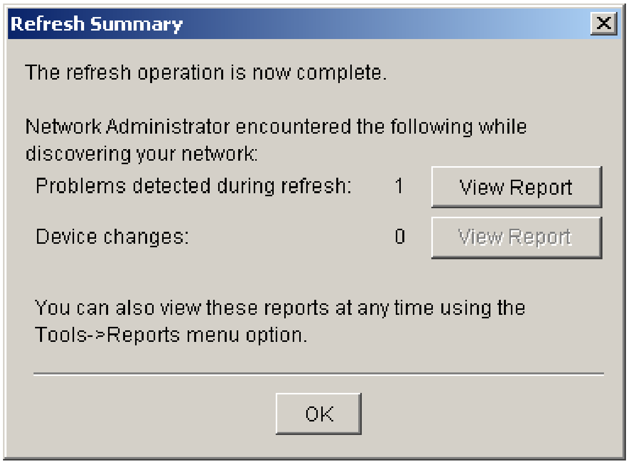
The refresh operation itself may be started by one of several actions as follows:

- **Immediately after an import operation** — after a successful import, a refresh is performed automatically on the imported devices before they are added to the inventory. In this case the *Progress* dialog is shown in 'restored' form.
- **By manually invoking the refresh operation** — if you select one or more devices in the device list and choose *Device* > *Refresh*, the refresh operation will be started on the selected devices. The *Progress* dialog is shown in 'restored' form.
- **When a scheduled refresh is run** — you can schedule an automated refresh to occur at some point in the future or at regular intervals. You can control the schedule from the *Options* > *Refresh* menu. This option also uses the minimized version of the Refresh *Progress* dialog.

## Refresh Summary Dialog

The *Refresh Summary* dialog displays either after the *Refresh Progress* dialog completes or if you select *Update* after an automated refresh completes as shown in Figure 46.

**Figure 46** Refresh Summary Dialog



Refresh Summary

The refresh operation is now complete.

Network Administrator encountered the following while discovering your network:

Problems detected during refresh: 1

Device changes: 0

You can also view these reports at any time using the Tools->Reports menu option.

The *Refresh Summary* dialog provides you with the following information:

- **Problems detected during importing** — displays if the refresh was run as a result of performing an import operation. It also allows you to view the Import report. For more information on problems that can occur see "Import Problems" on page 102.
- **Problems detected during refresh** — shows the number of refresh problems and you can also view the Refresh report. This line is absent if an import was performed but no devices were successfully imported (in order to be able to run the refresh operation). In this case the dialog is still shown so that you can view the Import report.
- **Device changes** — displays if a refresh successfully completed on a previously non-empty inventory. You can view the Changes report to see the details of the changes.

## Import and Refresh Reports

The following reports are produced through the Importing and Refreshing feature:

### Import Report

The Import Report lists all devices that were successfully imported and passed onto the refresh operation. It also includes any problems encountered, such as invalid CSV record entries or problems connecting to the HP OpenView database. For more information on the type of problems encountered see "Import Problems" on page 102.

*If you cancel a refresh operation after the import operation has completed you can still view the import report from the* History *tab of the* Main Reports *dialog.*

### Refresh Report

The Refresh Report lists all the problems encountered during the refresh operation, such as the device not responding. For more information on the types of problem encountered see "Refresh Problems" on page 103.

### Changes Report

The Changes Report lists any changes that were detected for devices that existed in the inventory file prior to performing the refresh.

From the *Refresh Summary* dialog you can view each of these reports (where applicable). Additionally, once a report has been generated it can also be viewed from the *History* tab of the *Main Reports* dialog. The reports are automatically generated in the background as part of the import/refresh process. You do not need to view the reports from the *Summary* dialog for them to be added to the Report history.

## Examples

The following section provides examples of how you might use the import and refresh operations.

### Importing Newly Discovered Devices from HP OpenView

One of your sites has expanded and requires some new users to be connected to the network. As a result, you have added some new 3Com switches to the appropriate subnet in order to handle the extra connections. You are running HP OpenView and it has detected the new devices on your network.

To use the configuration tools provided by 3Com Network Administrator on new devices, you must import them into a 3Com Network Administrator inventory file:

1. Launch the *Import* dialog by selecting the *File* > *Import* menu.
2. Ensure that the *Import From HP OpenView* radio button is selected (it is selected by default) and click *OK*.
3. A list of subnets displays. Select the subnet to which you have added the new device and click *OK*.
4. The *Import Progress* dialog displays indicating that it is importing the devices on your selected subnet. After a while the *Import Progress* dialog will close and be replaced by the *Refresh Progress* dialog listing the existing devices in the subnet. The new devices will appear as each one is successfully refreshed.
5. When the refresh completes, the *Summary* dialog displays and should indicate that there were no import or refresh problems. If there are any, try to resolve them. For further information on how to do this see "Key Considerations" on page 102.
6. Close the *Summary* dialog and the new devices are added to the inventory. Confirm this by selecting the relevant subnet in the tree. The devices appear in the device list shown in the device window.
7. You can now use the configuration tools that 3Com Network Administrator provides to manage the new devices.

## Importing Devices from a Spreadsheet

You maintain the list of devices on your network in a Microsoft Excel spreadsheet. You wish to configure the devices using the tools provided by 3Com Network Administrator.

To enable access to the configuration tools that 3Com Network Administrator provides you must export the devices from your spreadsheet to a CSV file and then import them into your 3Com Network Administrator inventory file. One of the columns in the spreadsheet must specify the IP address of the device:

1. Open your spreadsheet in Microsoft Excel.
2. Keep the main spreadsheet open and create a second spreadsheet by selecting *File* > *New*.
3. Use the *Window* menu to return to the main spreadsheet and select the entire *IP Address* column by clicking on the column header to highlight it.
4. Select *Edit* > *Copy* to copy the highlighted column.
5. Using the *Window* menu, return to the second spreadsheet.
6. Click the column header A to select the entire column and select *Edit* > *Paste* to paste the IP addresses into column.
7. Repeat this process for the *Subnet Mask* column, pasting it into column B of the second spreadsheet. If you have no subnet mask column in your main spreadsheet then leave column B blank in your second spreadsheet.
8. Repeat this process for the *Name* column, pasting it into column C of the second spreadsheet. If you have no name column in your main spreadsheet then leave column C blank in your second spreadsheet.
9. Repeat this process for the *Read Community* column, pasting it into column D of the second spreadsheet. If you have no read community column in your main spreadsheet then leave column D blank in your second spreadsheet.
10. Repeat this process for the *Write Community* column, pasting it into column E of the second spreadsheet. If you have no write community column in your main spreadsheet then leave column E blank in your second spreadsheet.
11. Select *File* > *Save As* to save the second spreadsheet and select *CSV* as the file type. Save the spreadsheet as **`C:\MyDevices.csv`**.

You are now ready to import the devices into 3Com Network Administrator:

**12** Launch 3Com Network Administrator if it is not already running.

**13** Select *File* > *Import*.

**14** Select the *Import From CSV File* radio button and enter `C:\MyDevices.csv` into the edit field.

**15** Select *OK*.

The *Import Progress* step is displayed indicating that 3Com Network Administrator is importing the devices from your CSV file. After a while the *Import Progress* dialog will close and be replaced by the *Refresh Progress* dialog. You will see the devices appearing in the list box.

**16** When the refresh completes the *Summary* step is displayed and should indicate that there were no import or refresh problems. Problems that have been detected should be resolved. For more information on how to do this see "Key Considerations" on page 102.

**17** Click *OK* in the *Summary* step and the new devices will be added to the inventory. Confirm this by selecting *All 3Com devices* in the tree. The devices will be present in the device list shown in the right hand side of the device window.

You can now use the configuration tools that 3Com Network Administrator provides to manage the imported devices.

## Refreshing Existing Devices

You are using Switch 4400s at the edge of the network and you need to increase the number of ports to connect some new users. To achieve this you have added extra units to a selection of your devices, creating stacked devices.

Certain configuration tools within 3Com Network Administrator can adapt to the fact that the configuration held in the inventory does not match that of the real devices. However, other configuration tools will either continue to function (warning you that the configuration is out of date) or will simply not function. 3Com recommends that you keep the configuration of devices held in the inventory file up-to-date with the real configuration on the network. Therefore, if you know certain devices are out-of-date you can refresh them as follows:

1 Select the *All 3Com devices* folder in the tree.

2 In the device list, select the devices that you have changed.

3 From the right-click menu, select *Refresh Information* to display the *Refresh Progress* step. The devices you have selected will appear in the list box each time one is successfully refreshed.

4 When the refresh completes the *Summary* step displays and should indicate that there were no refresh problems. Problems that have been detected should be resolved. For more information on how to do this see "Refresh Problems" on page 103.

5 Close the *Summary* step and the refreshed devices will now reflect their true configuration. You can confirm this by selecting one of the devices in the device list and select the *Device* > *Properties* menu to launch the *Properties* dialog.

You can now use the configuration tools that 3Com Network Administrator provides to manage the refreshed devices.

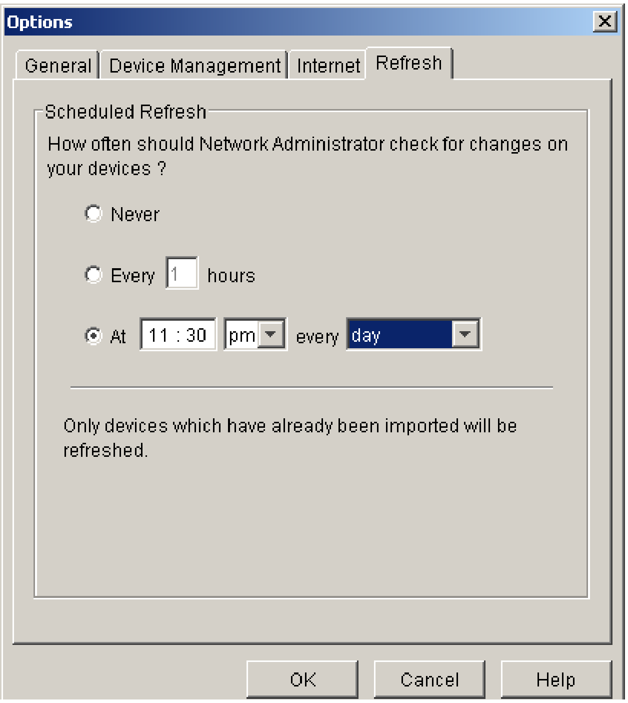
## Delaying Refreshing Existing Devices

You have an engineer working in a remote site who is making changes to the device configurations and these changes are likely to continue after you have left the office. You wish to be able to view the changes when you return to the office the following day. To do this:

1 Launch the *Options* step from *Tools* > *Options* and select the refresh pane.

2 From the *Refresh* tab in the step, schedule the refresh to run at *11.30pm* and from the drop-down list select *day* as shown in Figure 47:

**Figure 47** Refreshing



Options

General | Device Management | Internet | Refresh

Scheduled Refresh

How often should Network Administrator check for changes on your devices ?

○ Never

○ Every 1 hours

● At 11 : 30 pm every day

Only devices which have already been imported will be refreshed.

3. Ensure that 3Com Network Administrator is left running on your PC before you leave the office.
4. When you return the next day the *Update* button is enabled. Select *Update* and the *Summary* step displays. You can review the changes on the devices by examining the Changes report which is available from the *Summary* dialog.
5. Close the *Summary* step and the refreshed devices will now reflect their true configuration.

*The Changes report is available at any time from the* Reports *dialog.*

*3Com recommends that you cancel this task upon completion otherwise the task will automatically run every day.*

## Key Considerations

The following section provides assistance with Importing and Refreshing.

### Import Problems

Any problems that are encountered during importing are listed in the Import report. These will either relate to problems met when parsing the CSV file or problems met when attempting to read information from the HP OpenView database. Typically, there should be few problems importing from the HP OpenView database.

#### Problems Importing from CSV

The following is a list of potential problems (and suggested solutions) that may be encountered when importing from a CSV file. If the import operation encounters any of these problems they will be listed in the Import report.

- **The IP address was missing or invalid for a given record** — the IP address must be present and of the correct format for each device record in the CSV file. The expected format is standard dotted decimal. For example, `nnn.nnn.nnn.nnn`, where `nnn` is a decimal value between 0 and 255.

  If the IP address is not in the correct format, the whole line will be rejected and the device will not be added to the inventory.

- **The name field contains invalid characters** — 3Com Network Administrator only supports device names which contain characters within the ASCII range 32 to 126.

  Any name containing characters outside this range will have those characters converted to question mark ('?') characters. The device record is not rejected but is passed on to the refresh operation for further validation.

- **The community string field contains invalid characters** — 3Com Network Administrator only supports community strings which contain characters within the ASCII range 32 to 126.

  If a community string is encountered that contains characters outside of this ASCII range, the characters will be converted to question marks ('?'). The device record is not rejected but is passed on to the refresh operation for further validation. This applies to both the read community and write community fields.

### Problems Importing from HP OpenView

If you encounter problems importing from HP OpenView, ensure that you have HP OpenView services running so that 3Com Network Administrator can connect to the HP OpenView database.

If the import operation encounters this problem it will be reported in the Import report.

## Refresh Problems

Any problems encountered during refresh are listed in the Refresh report. These all relate to problems encountered when reading live information from the devices on the network.

- **Devices did not respond to a ping** — if this occurs:

  - During a refresh operation which is running as a result of an import, the device will not be added to the inventory.
  - During a refresh on a device already in the inventory, its details will not be modified.

  Check that the part of the network to which the device is attached is accessible from your workstation. From the command prompt, try pinging the device and its neighboring devices. The *Tracert* command may also help in determining where the problem is in trying to contact the device.

- **Failed to establish the device as being a 3Com device** — a failure can occur if:

  - *The device did not respond to SNMP* — this is most likely due to the read community string being incorrect. It was either incorrectly specified in the CSV file or (if importing from HP OpenView) it has changed since it was last discovered in HP OpenView.
  - *The device responded to SNMP but was detected as being a non-3Com device* — this is either because you inadvertently included a non-3Com device in the CSV file or (if importing from HP OpenView) you have replaced the device since it was last discovered in HP OpenView.

  In either case, if this was detected during a refresh operation as a result of an import, the device will not be added to the inventory. If this was a refresh on a device already in the inventory, its details will not be modified.

- **Failed to verify the write community string** — 3Com Network Administrator attempts to validate the write community string supplied to the refresh operation. As a last resort, if the refresh operation fails to verify the supplied write community, it will try to use the factory defaults for the given device. This may fail if:

  - No write community string was supplied from the CSV file or the HP OpenView database and the write community has changed to something other than the factory default.

  - An incorrect write community string was supplied from the CSV file or the HP OpenView database and the write community has been changed to something other than the factory default.

  In either case the device will still be added to the inventory. However, tools which subsequently require 'write access' to the device will not operate correctly.

- **Error encountered while reading information from the device** — typically, this will be due to loss of communication when reading detailed information from the device. This will not prevent the device from being added to the inventory, although some of its details may be incorrect. When the refresh operation completes, attempt a manual refresh on the problem device(s). If the problem persists it may be that your network is heavily congested.

- **Unsupported agent detected** — 3Com Network Administrator only supports software versions from a minimum revision. Although it will accept the device, some of its details may be incorrectly displayed and some of the administrative tools may function incorrectly. The Refresh report will indicate the minimum version for the given device type. 3Com recommends that you update the device to be at least the minimum supported version.

- **Port Self Test Failure** — this will not affect the operation of 3Com Network Administrator although it draws attention to a potential problem with the device itself.

## Updating the Inventory

When the refresh operation completes the *Summary* dialog is displayed.

*The* Summary *dialog is not displayed if the operation was run as a scheduled refresh and it completed with the* Progress *dialog in its minimized form. Instead the* Update *button becomes enabled and when it is clicked will display the* Summary *dialog.*

When the *Summary* dialog is closed the inventory is updated with the new information.

If you are updating the inventory you should be aware of the following rules:

- If a new device was successfully refreshed as a result of an import operation it will be added to the inventory.
- If an existing device was refreshed and found to have changed configuration (for example, a unit was added), then the inventory will be updated to reflect the new configuration.
- If an attempt was made to refresh an existing device but the device did not respond (or it was found to no longer be a 3Com device) then it will not be removed from the inventory. The information held for that device will remain unchanged and a warning will be given in the Refresh report.
- Devices are never deleted from the inventory by the refresh operation. The exception to this is if two separate devices (with distinct IP addresses) are combined (using stacking) to form a single device. In this case, one of the devices will be deleted and the other updated to reflect the combined new configuration.

## Subnet Creation

Prior to being added to the inventory, the devices are sorted into the subnets they belong to. These subnets appear in the group tree on the device window. Subnets are not created using the subnet information provided by the import (for example, the subnet mask in the CSV record). Instead, the subnet masks obtained from the devices during refresh are used.

Subnets are only created based on a device's primary IP address (supplied during import) and its corresponding subnet mask.

For example, consider a router that has two interfaces:

192.168.1.1/24 and 192.168.2.1/24

If you only include the first address in the CSV file then only the 192.168.1.0 subnet will be created in the inventory. However, if you include the second address or the address of another device on the 192.168.2.0 subnet, then both subnets will be created in the inventory and the router will appear in both subnet groups.

## Frequently Asked Questions

### The device I imported was not added to the inventory file

- Check the Import report to ensure the device was not rejected due to an invalid CSV entry or due to it not appearing as a 3Com device in HP OpenView.
- Check the Refresh report to ensure there were no errors when refreshing the given device.

### The Refresh report says that my device is not a 3Com device but I am certain that it is

Verify that you can communicate with the device using the read community string you supplied to the import, by reviewing the CSV file or the information held in HP OpenView.

# 6 BACKUP, RESTORE AND SETUP

## Overview

This chapter describes how 3Com Network Administrator can be used to manage the software configuration of the 3Com devices on your network.

You can use Backup, Restore and Setup to:

- Save the software configuration of your 3Com devices.
- Apply a software configuration, saved in the backup file, to either the device from which it originated or to a replacement device of the same type.
- Copy the software configuration of one 3Com device to other devices of the same type.

The following topics are covered in this chapter:

- Key Concepts
- Backup Components
- Restore Components
- Setup Components
- Examples
- Useful Information and References
- Key Considerations

## Key Concepts

The Backup feature is designed to help you store the software configuration of your 3Com devices. The Backup feature associates each saved backup with the source device from which the backup was taken, by generating a unique physical identification for the source device.

The Restore feature allows you to apply a saved backup either to the device matching the physical identification associated with the backup (the source device) or if the source device cannot be found on your network, you can apply the saved backup to a replacement device. The replacement device must have the same physical configuration as the source device it is replacing.

The Setup feature enables you to apply a software configuration from either a saved backup or a 'live' network device to a set of target devices that have the same physical configuration as the source device.

### Physical Identification of Devices

Every backup file is associated with a physical identification that uniquely identifies the source device from which the backup was taken. This physical identification is derived from the hardware address of the source device.

*The physical identification of a device, made up of more than one unit, is unique to that combination of units. The physical identification of a device will change if you replace or re-arrange the order of the units.*

### Physical Configuration of Devices

Every backup file contains a description of the physical configuration of the source device, constructed as follows:

- The physical configuration is determined from the devices' type (part number) and the media type of each of its ports.
- If the physical configuration is made up of more than one unit, it will include the type and position of each unit in the device.
- The physical configuration includes the type of any plug-in modules (including intelligent modules) that are present in the device.

*The Restore and Setup Wizards identify potential target devices in the current inventory file as those that match the physical configuration of the source device. 3Com recommends that you refresh the current inventory file prior to using Restore or Setup, unless you are sure that there have been no changes to the physical configuration of the devices on your network.*

## Backup Components

This section describes how to use the Backup feature of 3Com Network Administrator.

### Device Backup Wizard

You can create and manage backup files for any of the supported 3Com devices on your network.

*Select* Device > Backup *to open the Device Backup Wizard.*

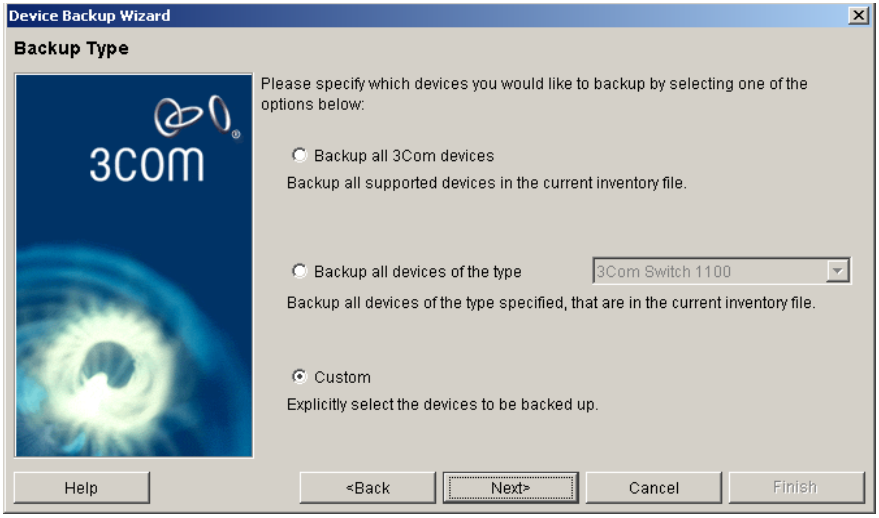
Within the Device Backup Wizard you can:

- Select a group of devices to back up
- Enter a label and description to be applied to all of the backup files created by the operation
- Schedule the backup operation to take place at a particular time and date

#### Backup Type Step

From the *Backup Type* step you can select which of the supported 3Com devices in your network you wish to back up as shown in Figure 48:

**Figure 48** Device Backup Wizard - Backup Type



Device Backup Wizard

**Backup Type**

Please specify which devices you would like to backup by selecting one of the options below:

○ Backup all 3Com devices

Backup all supported devices in the current inventory file.

○ Backup all devices of the type 3Com Switch 1100

Backup all devices of the type specified, that are in the current inventory file.

● Custom

Explicitly select the devices to be backed up.

The options are:

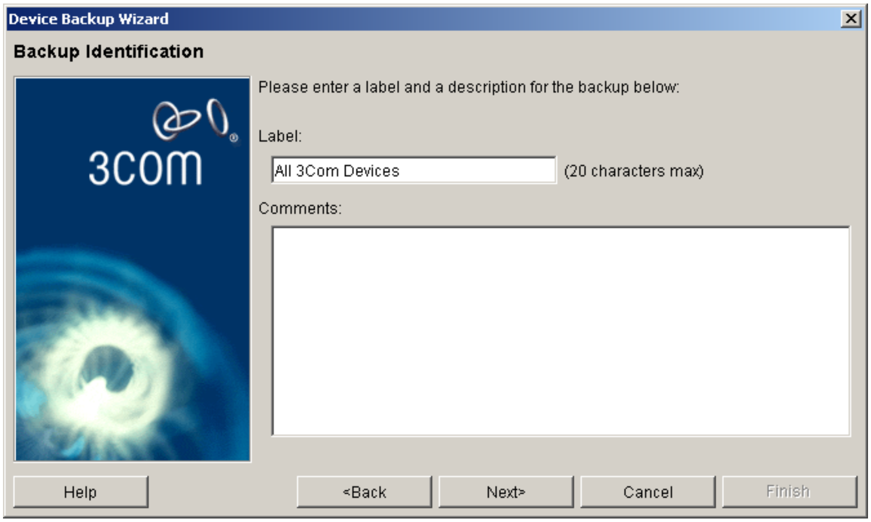
- **Backup all 3Com devices** — backs up all of the supported 3Com devices in the current inventory file. 3Com recommends that you use this backup type on the first occasion that you use the Device Backup Wizard. By choosing this backup type you will ensure that you have a saved configuration for all your supported devices.
- **Backup all devices of the type** — backs up all devices of the specified type in the current inventory file. You may wish to use this backup type after adding and configuring a large number of devices of a particular type on your network.
- **Custom** — which allows you to choose which of the supported 3Com devices in your network you wish to back up. 3Com recommends that you backup any major change you make to the configuration of your devices.

*The wizard uses your current selection from the inventory file as the basis for the custom selection.*

### Specify Devices to Backup Step

You can manage your device configuration backups by labelling your backups and providing comments for them as shown in Figure 49.

**Figure 49** Device Backup Wizard - Backup Identification



Please enter a label and a description for the backup below:

Label:

All 3Com Devices (20 characters max)

Comments:

You must provide a label, using a maximum of 20 characters, to be associated with all backups created by the current backup operation. You can, if you wish, provide a longer description of the backups in the comments field in this step. The label and comments you provide will be used during future Restore and Setup operations to help you identify the backups.

*The wizard will not progress to the next step until a label has been entered, although the comments are optional.*

### Scheduling Step

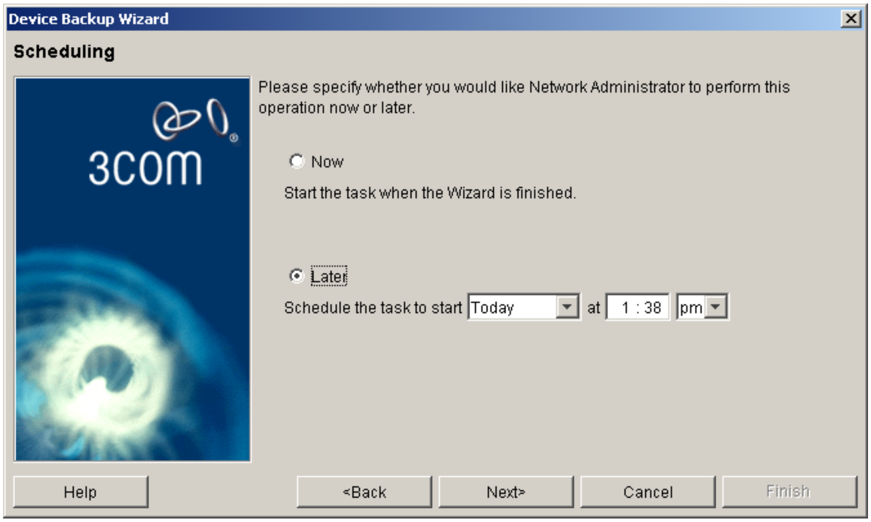
You can choose the operation schedule as either:

- **Now** — if you want the Device Backup operation to begin as soon as you complete the wizard

  Or

- **Later** — if you want the Device Backup operation to begin at a later time. The time field is in 12-hour format so remember to set to am/pm. You can use the day and time fields to schedule the operation to begin up to a week ahead as shown in Figure 50:

**Figure 50** Device Backup Wizard - Scheduling



Device Backup Wizard

Scheduling

Please specify whether you would like Network Administrator to perform this operation now or later.

○ Now

Start the task when the Wizard is finished.

● Later

Schedule the task to start Today at 1 : 38 pm ℹ *You can review or cancel a scheduled Device Backup operation from the* Scheduled Tasks *dialog which can be launched from* Tools > Scheduled Tasks.

### Summary Step and Progress

Unless you have chosen to schedule the Device Backup operation for a future date, the operation begins once you have selected *Finish* on the *Summary* step.

During the Device Backup operation, the *Device Backup Progress* dialog is shown to indicate the progress of the operation.

ℹ *The* Device Backup Progress *dialog can be 'minimized' to the status bar of the application. If the Device Backup operation started according to a schedule, then it will appear in its minimized state.*

ℹ *You can cancel the Device Backup operation at any time. If you do cancel the operation then any backups that have already successfully completed will be kept.*

## Device Backup Events

An alarm will be generated in HP OpenView for each device that you attempt to back up. The alarm source is the IP address of the device and both the alarm severity and the alarm message indicate whether the attempt to back up the device was successful. The detail of the alarm message for a successful backup includes the label that was applied to the backup. The detail of the alarm message for an unsuccessful backup describes what went wrong.

ℹ *If you choose to cancel a Device Backup operation before it is complete, no alarms will be generated for devices that are still pending or in progress at that time.*

## Device Backup Reports

The following reports relate to the Device Backup feature:

### Backup Summary Report

When the Device Backup operation completes, the Backup Summary report is automatically generated. You can choose whether to view the report or not from the *Device Backup Summary* dialog shown at the end of the operation.

The Backup Summary report details the following:

- The label and description applied to all of the successful backups created by the Device Backup operation.
- The devices for which a backup was successfully created. A hyperlink to the saved backup file for each device is created. See "Backup Files" on page 114 for more details.
- The devices that could not be backed up. 3Com Network Administrator reports a reason for each failure.

*You can view the Backup Summary report at any time after the operation has completed from the* History *tab of the* Reports *dialog, launched from* Tools > Reports.

### Backup Audit Report

The Backup Audit report determines how recently the devices on your network have been backed up and which devices have not yet been backed up.

*You can generate a Backup Audit report at any time from the* Generate Reports *tab of the* Reports *dialog, launched from* Tools > Reports.

The Backup Audit report lists the following:

- The devices on your network that have one or more backups available. A hyperlink to the most recently saved backup file for each device is provided, see "Backup Files" on page 114 for more information.
- The 3Com devices on your network that have no backups associated with them. For devices that are not supported by Backup, Restore and Setup, 3Com Network Administrator provides further details on the reason why.

### Backup Files

The Device Backup operation creates a new backup file each time it successfully saves the configuration of a device. You can view the contents of a backup file by:

- Clicking *Label* in the Backup Audit report to view the most recent backup file for any device in the current inventory file.
- Clicking *View Backup* in the Backup Summary report to view the backup file created by the corresponding Device Backup operation.
- Locating a backup file on your hard disk and opening the file directly using your web browser. See "Managing Backup Files" on page 132 for details on how to do this.

See "Understanding Backup Files" on page 132 for an explanation of the contents of your backup files.

*Backup files are best viewed using Microsoft Internet Explorer 5.0 (or later). 3Com strongly recommends that you do not edit the contents of any backup files.*

## Restore Components

This section describes how to use the Restore feature of 3Com Network Administrator.

### Device Restore Wizard

You can apply a saved backup to either the device from which the backup was taken or to a replacement device that has the same physical configuration.

The Device Restore Wizard must be launched against the selection of a single device in the current inventory file. The selected device will be the target of the Restore operation.

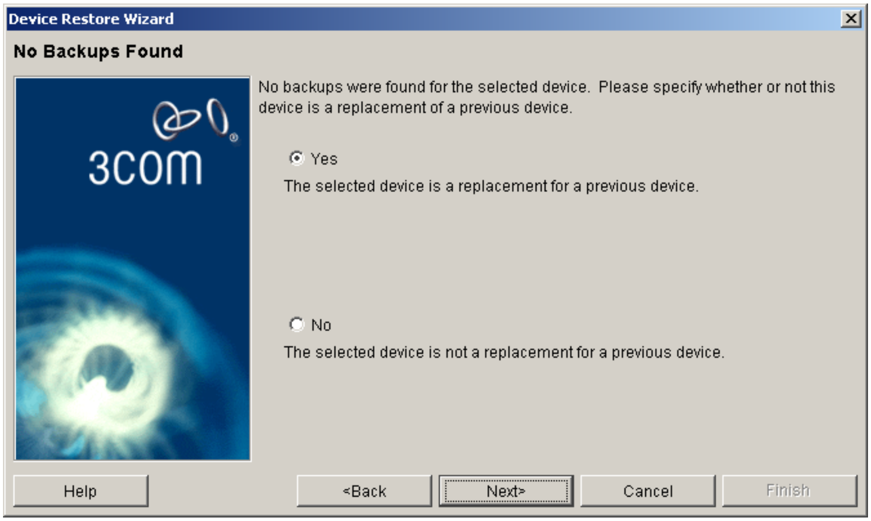
You can select from the saved backups that have the same physical configuration as the target device. If there are no saved backups associated with the target device because it is a replacement device, you will be given the opportunity to specify the device that this is a replacement for.

*The Device Restore Wizard is launched from* Device > Restore.

## No Backups Found Step

When you launch the Device Restore Wizard against a target device that has no backup files associated with it, the wizard shows the *No Backups Found* step as shown in Figure 51. The wizard will ask you whether the target device is a replacement for another device.

**Figure 51** Device Restore Wizard - No Backups Found



No Backups Found

No backups were found for the selected device. Please specify whether or not this device is a replacement of a previous device.

● Yes

The selected device is a replacement for a previous device.

○ No

The selected device is not a replacement for a previous device.

If your target device is not a replacement for another device and there are no backup files associated with your target device, the Device Restore Wizard cannot continue. The Restore operation can only be used to apply a saved backup to either the device from which it originated or to a replacement for the device.

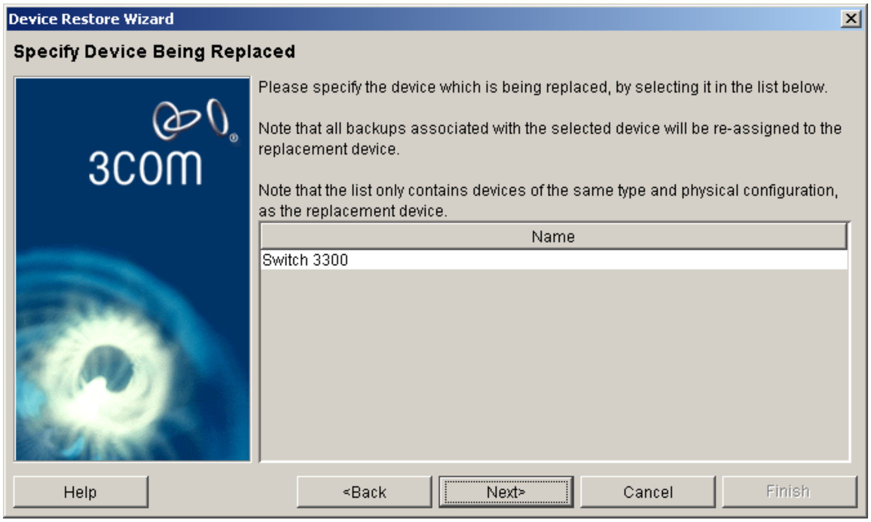
*If you want to apply a 'saved' configuration to a device which is neither the source of the backup nor a replacement for the source of the backup, then you should use the Device Setup Wizard. See "Device Setup Wizard" on page 119 for more details.*

## Specify Device Being Replaced Step

When you indicate in the *No Backups Found* step that the target device is a replacement for another device, the *Specify Device Being Replaced* step is shown. This step is only shown if there is at least one backup from another device with the same physical configuration as your target device.

You must select the device that has been replaced by your target device from the table, as shown in Figure 52.

**Figure 52** Device Restore Wizard - Specify Device Being Replaced



Device Restore Wizard

Specify Device Being Replaced

Please specify the device which is being replaced, by selecting it in the list below.

Note that all backups associated with the selected device will be re-assigned to the replacement device.

Note that the list only contains devices of the same type and physical configuration, as the replacement device.

| Name |
|---|
| Switch 3300 |

The table shows the name of all devices that have one or more existing backups and have the same physical configuration as your target device. The list of devices is taken from the saved backup files. The device that is being replaced does not have to be present in the current inventory file.

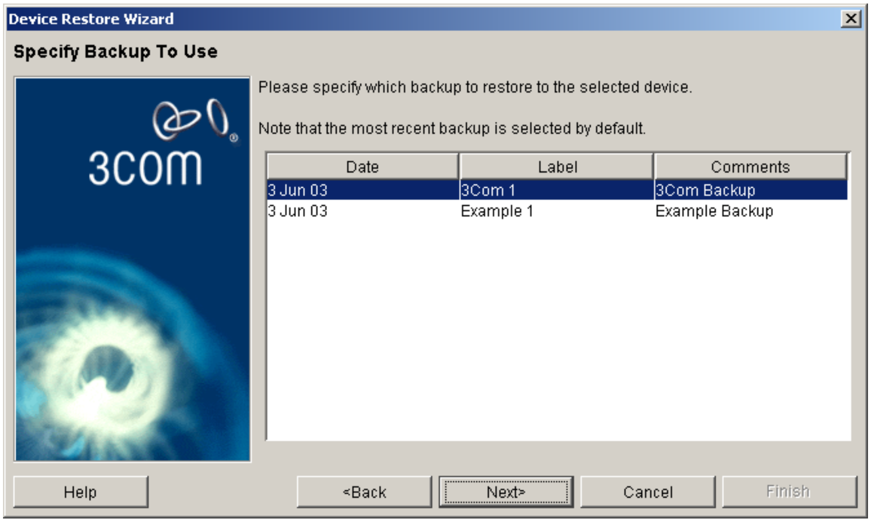
Once you have specified the device that has been replaced, all existing backups for that device will be associated with the target device after the Device Restore operation has completed successfully.

### Specify Backup to Use Step

If the target device has one or more existing backup files associated with it, the *Specify Backup To Use* step is displayed. The wizard also shows this step after the *Specify Device Being Replaced* step.

The *Specify Backup To Use* step shows a table of existing backups associated with either the target device or the device that has been replaced, as shown in Figure 53.

**Figure 53** Device Restore Wizard - Specify Backup To Use



Device Restore Wizard

Specify Backup To Use

Please specify which backup to restore to the selected device.

Note that the most recent backup is selected by default.

| Date | Label | Comments |
|---|---|---|
| 3 Jun 03 | 3Com 1 | 3Com Backup |
| 3 Jun 03 | Example 1 | Example Backup |

The table provides the following information about each backup to help you identify the one to apply to the target device:

- **Date** — the date on which the backup was created.
- **Label** — the label you gave this backup in the Device Backup Wizard.
- **Comments** — the comments that you gave this backup in the Device Backup Wizard.

You must select a backup to apply to the target device before proceeding to the final step of the wizard.

### Summary Step and Progress

Once you select *Finish* on the *Summary* step the Device Restore operation is ready to begin.

Before any configuration takes place, the Device Restore operation displays a warning dialog. The dialog advises you to ensure that the target device is isolated from your network before proceeding. You must acknowledge this warning before continuing. See "Key Considerations" on page 133 for further information.

During the Device Restore operation, the *Device Restore Progress* dialog is shown to indicate the progress of the operation.

*The* Device Restore Progress *dialog can be 'minimized' to the status bar of the application by clicking* Minimize *in the bottom left hand corner of the* Progress *dialog.*

*You can cancel the Device Restore operation at any time. If you do cancel the operation then the configuration of the target device may be left in an inconsistent state.*

## Device Restore Event

An alarm will be generated in HP OpenView for the Device Restore operation. The alarm source is the IP address of the target device and both the alarm severity and the alarm message indicate whether the attempt to restore the saved software configuration to the device was successful. The detail of the alarm message for a successful operation includes the label of the backup that was applied to the target device. The detail of the alarm message for an unsuccessful operation describes what went wrong.

*You can view the Restore Summary report at any time after the operation has completed from the* History *tab of the* Reports *dialog, launched from* Tools > Reports.

## Restore Summary Report

When the Device Restore operation completes, the Restore Summary report is automatically generated. You can choose to view the report from the *Device Restore Summary* dialog that is shown at the end of the operation.

The Restore Summary report details the following:

- The label and description of the saved backup that the Device Restore operation attempted to apply to the target device.
- The details of the target device for the operation
- The result of the Device Restore operation including a further explanation where appropriate.

*You can view the Restore Summary report at any time after the operation have completed from the* History *tab of the* Reports *dialog, launched from* Tools > Reports.

## Setup Components

The following section describes how to use the Device Setup feature of 3Com Network Administrator.

### Device Setup Wizard

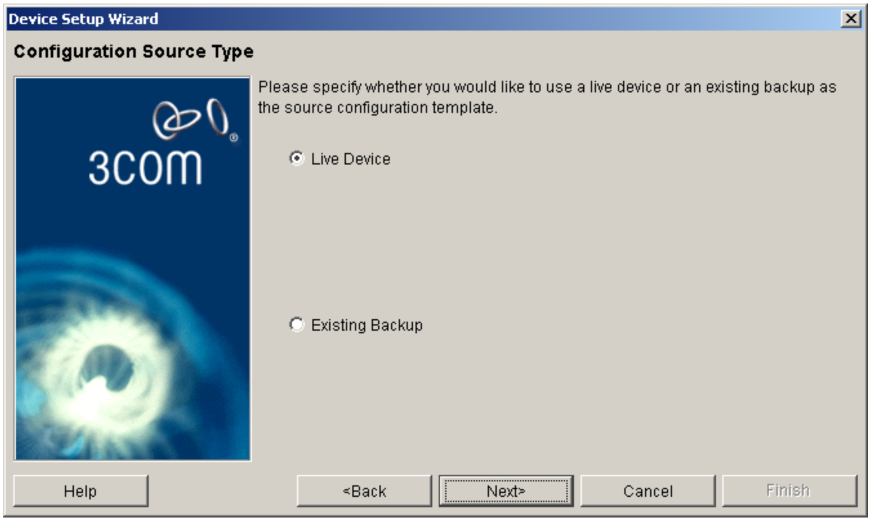
You can apply a software configuration to one or more target devices. The software configuration you choose to apply to the target device can be either the software configuration of a device on your network or a software configuration saved in a backup file. The target device (or devices) you choose to set up must have the same physical configuration as the source device of the software configuration.

*The Device Setup Wizard can be launched from* Device > Setup.

#### Configuration Source Type Step

You can choose whether the software configuration that will be applied to your target devices should come from either a 'live' device on your network or a saved backup as shown in Figure 54.

**Figure 54** Device Setup Wizard - Configuration Source Type



Device Setup Wizard

Configuration Source Type

Please specify whether you would like to use a live device or an existing backup as the source configuration template.

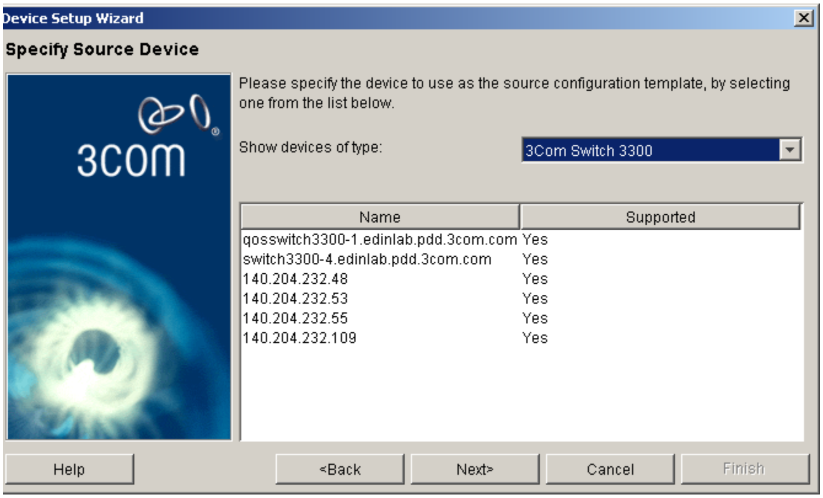
● Live Device

○ Existing Backup

#### Specify Source Device Step

When you choose to use a 'live' device on your network as the source software configuration, the Device Setup Wizard shows the *Specify Source Device* step as shown in Figure 55:

**Figure 55** Device Setup Wizard - Specify Source Device



Device Setup Wizard

**Specify Source Device**

Please specify the device to use as the source configuration template, by selecting one from the list below.

Show devices of type: 3Com Switch 3300

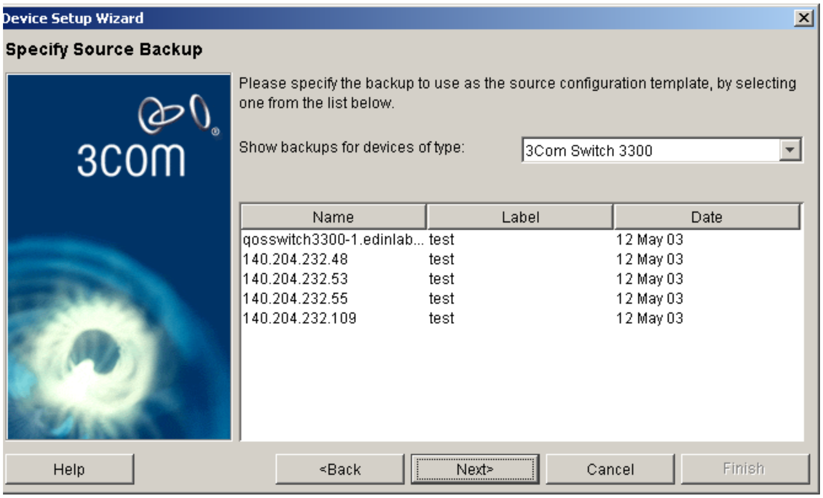
| Name | Supported |
|---|---|
| qosswitch3300-1.edinlab.pdd.3com.com | Yes |
| switch3300-4.edinlab.pdd.3com.com | Yes |
| 140.204.232.48 | Yes |
| 140.204.232.53 | Yes |
| 140.204.232.55 | Yes |
| 140.204.232.109 | Yes |

From this step you can select any one of the supported devices in the current inventory file. The device you select here will be used as the source of the software configuration applied to your target devices.

## Specify Source Backup Step

When you choose to use an existing backup as the source software configuration, the *Specify Source Backup* step as shown in Figure 56:

**Figure 56** Device Setup Wizard - Specify Source Backup



Device Setup Wizard

**Specify Source Backup**

Please specify the backup to use as the source configuration template, by selecting one from the list below.

Show backups for devices of type: 3Com Switch 3300

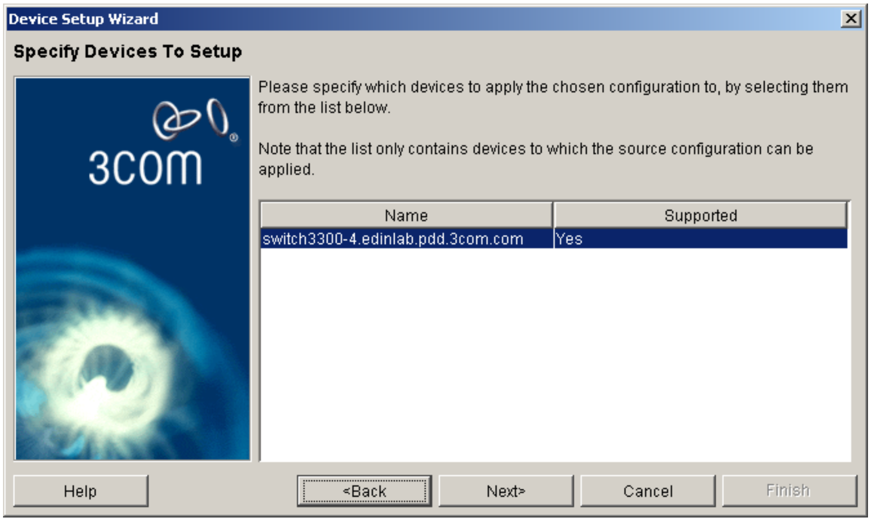
| Name | Label | Date |
|---|---|---|
| qosswitch3300-1.edinlab... | test | 12 May 03 |
| 140.204.232.48 | test | 12 May 03 |
| 140.204.232.53 | test | 12 May 03 |
| 140.204.232.55 | test | 12 May 03 |
| 140.204.232.109 | test | 12 May 03 |

From this step you can select any one of the backups you have created using the Device Backup operation. The backup you select here will be applied to your target devices.

## Specify Devices to Setup Step

This step presents all the supported devices in your current inventory file that have the same physical configuration as the source of the software configuration you have chosen to apply as shown in Figure 57:

**Figure 57** Device Setup Wizard - Specify Devices To Setup



Specify Devices To Setup

Please specify which devices to apply the chosen configuration to, by selecting them from the list below.

Note that the list only contains devices to which the source configuration can be applied.

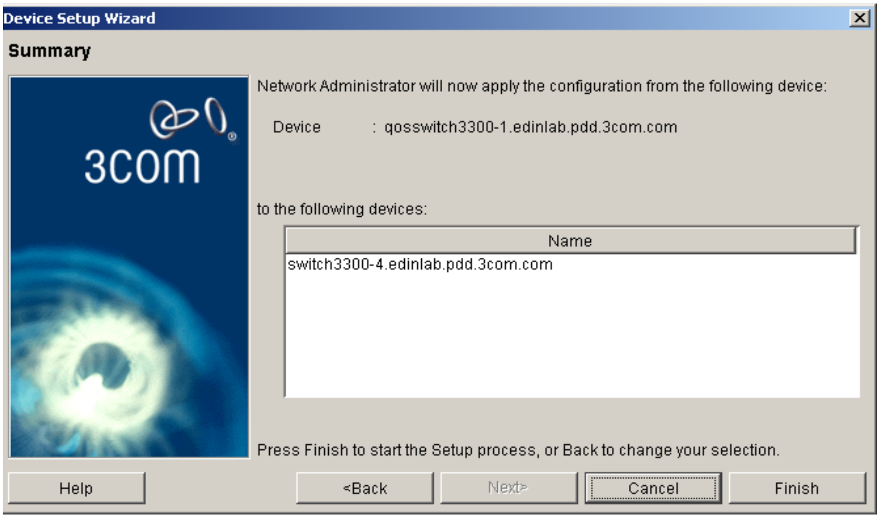
| Name | Supported |
|---|---|
| switch3300-4.edinlab.pdd.3com.com | Yes |

Select the target devices that you wish to apply the chosen software configuration to.

## Summary Step and Progress

The Device Setup operation is ready to begin once you select *Finish* on the *Summary* step as shown in Figure 58.

**Figure 58** Device Setup Wizard - Summary



Device Setup Wizard

Summary

Network Administrator will now apply the configuration from the following device:

Device : qosswitch3300-1.edinlab.pdd.3com.com

to the following devices:

| Name |
|---|
| switch3300-4.edinlab.pdd.3com.com |

Press Finish to start the Setup process, or Back to change your selection.

Before any configuration takes place, the Device Setup operation displays a warning dialog. The dialog advises you to ensure that the target devices are isolated from your network before proceeding. You must acknowledge this warning before continuing. See "Key Considerations" on page 133 for further information.

During the Device Setup operation, the *Device Setup Progress* dialog is shown to indicate the progress of the operation.

*The* Device Setup Progress *dialog can be 'minimized' to the status bar of the application by clicking* Minimize *in the bottom left hand corner of the Progress dialog.*

*You can cancel the Device Setup operation at any time. If you do cancel the operation then the configuration of the target device that is in progress at the time may be left in an inconsistent state. Any devices that have already been configured by the Device Setup operation prior to cancellation will keep their new configuration.*

## Device Setup Event

An alarm will be generated in HP OpenView for each device that 3Com Network Administrator attempts to configure as part of the Device Setup operation. The alarm source is the IP address of the device and both the alarm severity and the alarm message indicate whether the attempt to apply the source software configuration to the device was successful. The detail of the alarm message for a successfully configured device identifies the source device or backup that provided the software configuration. For devices that could not be configured, the detail of the alarm message describes what went wrong.

*If you choose to cancel a Device Setup operation before it is complete, no alarms will be generated for target devices that are still pending or in progress at that time.*

## Setup Summary Report

When the Device Setup operation completes, the Setup Summary report is automatically generated. You can choose whether to view the report or not from the *Device Setup Summary* dialog that is shown at the end of the operation.

The Setup Summary report covers the following:

- The details of the source device or backup that provided the software configuration.
- The devices that were successfully configured by the Device Setup operation.
- The devices that could not be configured by the Device Setup operation. 3Com Network Administrator reports a reason for each failure.

*You can view the Setup Summary report at any time after the operation has completed from the* History *tab of the* Reports *dialog, launched from* Tools > Reports.

## Examples

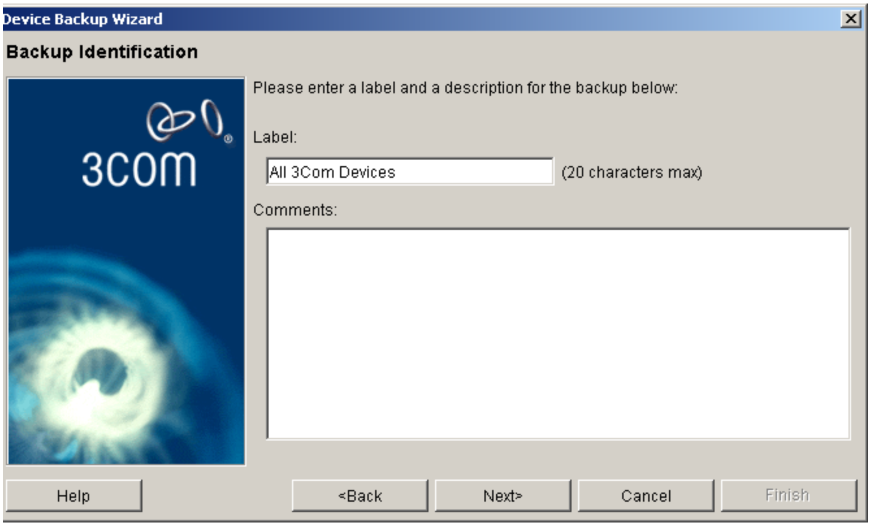
This section provides some examples of how to use Backup, Restore and Setup.

### Scheduling a Device Backup Operation

As part of your disaster recovery plan, you have decided that you need a backup of the software configuration of all devices on your network. You decide to schedule the operation to take place out of work hours to minimize the impact of the extra traffic on the network. To do this:

1. Ensure that all of the devices on your network are present in the current inventory file. You can check this by re-importing an updated device list from HP OpenView. See "Importing from HP OpenView" in Chapter 5 for further details.
2. Launch the Device Backup Wizard from the toolbar on the device window. Select *Next* on the *Introduction* step to display the *Backup Type* step as shown in Figure 48
3. Select the *Backup all 3Com devices* radio button to back up all of the supported 3Com devices in the network, then select *Next*.
4. The wizard displays the *Backup Identification* step, where you can enter a label and some comments that will help you to identify the backup if you ever need to restore a saved configuration as shown in Figure 59:

**Figure 59** Backup Identification Example



Please enter a label and a description for the backup below:

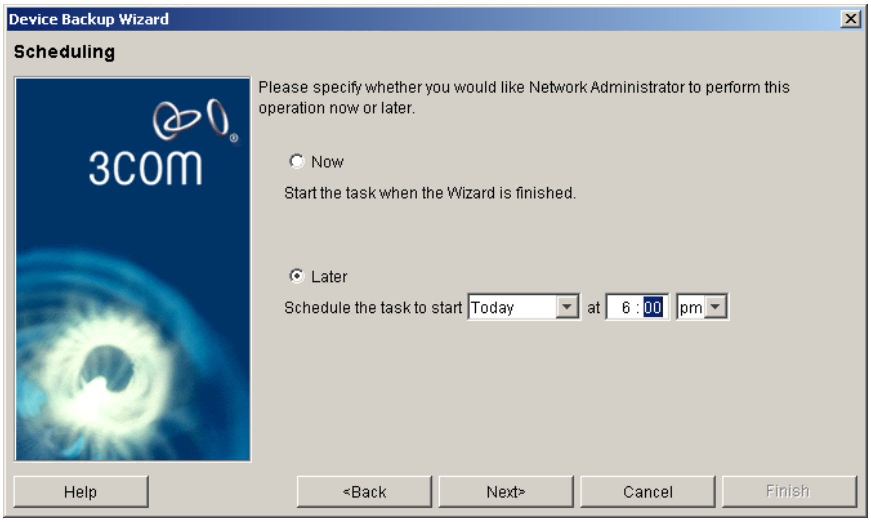
Label: All 3Com Devices (20 characters max)

Comments:

**5** Select *Next* to display the *Scheduling* step, then select the *Later* radio button to schedule the Device Setup operation to begin after you leave in the evening. Enter the time using the 12 hour clock (bearing in mind the setting for a.m./p.m.) and leave *today* as the selected day to run the operation as shown in Figure 60:

*If you decide to schedule the backup operation for a time after midnight, remember to set the date to the following day.*

**Figure 60** Scheduling Example



Device Backup Wizard

**Scheduling**

Please specify whether you would like Network Administrator to perform this operation now or later.

○ Now

Start the task when the Wizard is finished.

● Later

Schedule the task to start Today at 6 : 00 pm

**6** Select *Next* to display the *Summary* step and select *Finish* to schedule the Device Backup to start later in the evening. When the Device Backup operation runs, it will attempt to backup the software configuration of all the supported devices that are in the inventory file.

## Restoring to a Replacement Device

There has been a hardware failure on one of the core devices in your network. The failed device is one that you have earlier backed up as part of your disaster recovery plan. You have a replacement device with the same physical configuration as the failed device and you want to configure the replacement device and substitute it for the failed device.

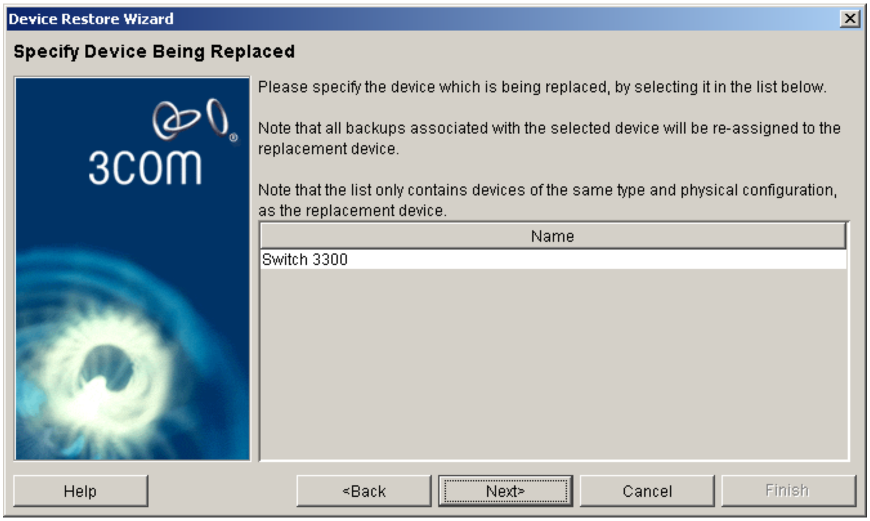
To do this:

1. If possible, keep the replacement device isolated from your network in a 'staging area'. Configure the replacement device with an IP address on the same subnet as your management PC. For further information on configuring a device with an IP address, refer to the user documentation that is supplied with your device.
2. Connect the management station to the replacement device using either a direct Ethernet connection or a connection through a simple hub or switch.
3. Create a new inventory and select *Add Device* to add the replacement device to the empty inventory file.

Add Device *can be launched from* Edit > Add Device.

4. Launch the Device Restore Wizard using the toolbar button on the main screen. Click *Next* from the *Introduction* step to display the *No Backups Found* step as shown in Figure 51.
5. Click the *Yes* radio button to indicate that the target device is a replacement for another device and click *Next* to display the *Specify Devices Being Replaced* step as shown in Figure 61:

**Figure 61** Specify Device Being Replaced Example



Device Restore Wizard

Specify Device Being Replaced

Please specify the device which is being replaced, by selecting it in the list below.

Note that all backups associated with the selected device will be re-assigned to the replacement device.

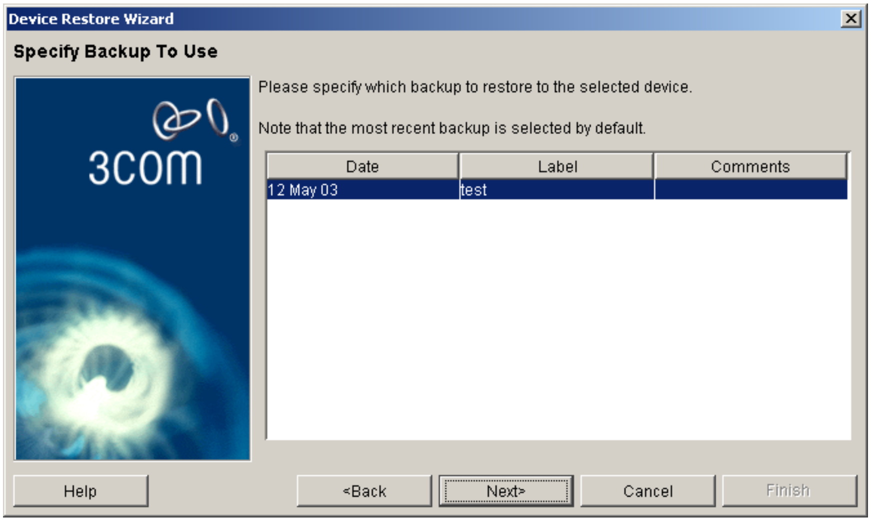
Note that the list only contains devices of the same type and physical configuration, as the replacement device.

| Name |
|---|
| Switch 3300 |

**6** Choose the name of the device that has suffered the hardware failure from the list of devices shown.

**7** Click *Next* to display the *Specify Backup To Use* step and select the most recent backup available for the failed device from the list of available backups as shown in Figure 62:

**Figure 62** Specify Backup To Use Example



Device Restore Wizard

Specify Backup To Use

Please specify which backup to restore to the selected device.

Note that the most recent backup is selected by default.

| Date | Label | Comments |
|---|---|---|
| 12 May 03 | test | |

**8** Click *Next* to display the *Summary* step and select *Finish* to start the Device Restore operation. You must wait until the operation has completed successfully. The Device Restore operation will automatically locate all of the existing backups for the failed device and re-associate them with the replacement device.

**9** Now that the replacement device has a suitable software configuration to be swapped in to the network, you can configure it with the IP address of the failed device. Disconnect the replacement device from the management station and swap it with the failed device to complete the task.

## Deploying a Group of Devices

You have decided to upgrade a large number of legacy switches at the edge of your network to Fast Ethernet devices. All of the new devices require the same port security and VLAN configuration and you would like to automate the process of configuring them. To do this:

1 If possible, keep the new devices isolated from your network in a ‘staging area’. Configure each of the devices with an IP address on the same subnet as your management PC. For further information on how to configure a device with an IP address, refer to the user documentation that is supplied with your device.

2 Configure one of the devices with the desired port security and VLAN settings. This will be referred to as the source device.

*By giving the source device an easily identifiable system name at this stage, you will be able to find the source device more easily when using the Device Setup Wizard.*

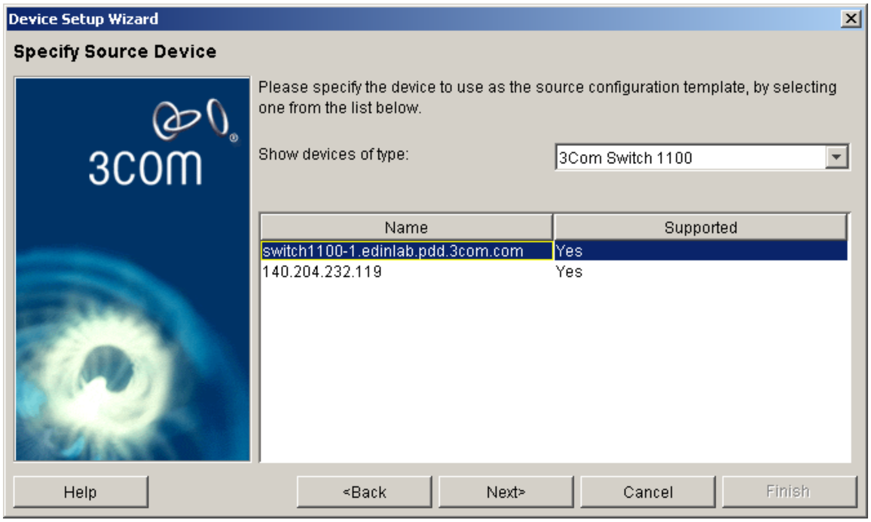
3 Connect the management station to all of the new switches using an Ethernet connection through a hub or switch.

4 Using the *Add Device* option or by importing the IP addresses from a CSV file, create a new inventory file and add the new switches to the inventory file. See “Importing from CSV Files” in Chapter 5 for more information.

5 Launch the Device Setup Wizard using the toolbar button on the main screen. Select *Next* at the *Introduction* step to display the *Configuration Source Type* step and select the *Live Device* radio button.

6 Select *Next* to display the *Specify Source Device* step and locate the source device in the table as shown in Figure 63:

**Figure 63** Specify Source Device Example



Device Setup Wizard

**Specify Source Device**

Please specify the device to use as the source configuration template, by selecting one from the list below.

Show devices of type: 3Com Switch 1100

| Name | Supported |
|---|---|
| switch1100-1.edinlab.pdd.3com.com | Yes |
| 140.204.232.119 | Yes |

7 Select *Next* to display the *Specify Devices to Setup* step and select all of the devices listed so that the configuration of the source device is applied to all the remaining new switches.

8 Select *Next* to display the *Summary* step and select *Finish* to start the Device Setup operation. You must wait until the operation has completed successfully.

9 Now that all of the new switches have the desired port security and VLAN settings, you can configure each of the switches with any individual settings that they require. You should also give each device the IP address that you will use to manage it once it has been added to your network.

10 Finally, disconnect the new devices from your management station and add them to the edge of your network. Once HP OpenView has discovered your new switches, you can re-import the 3Com Network Administrator inventory file in order to backup their configuration and perform other administrative tasks.

## Useful Information and References

The following section provides useful details related to Backup, Restore and Setup.

*The devices and agents supported by Backup, Restore and Setup are shown in Appendix A on page 241.*

### Supported 3Com Devices

The Device Backup, Restore and Setup Wizards determine which of the devices in your inventory file are supported. Backup, Restore and Setup can only be performed on supported devices. For devices that are not supported, the Backup Audit report and the *Summary* step on both the Device Backup Wizard and the Device Setup Wizard provide the reasons as follows:

- **Agent Update** — the device and all of its units or modules are supported, but one or more of the units or modules requires a more recent software version. See the "Agent Update Wizard" in Chapter 7 for instructions on how to update the agent software on your device.
- **License Required** — the agent software on the selected device is capable of providing Backup and Restore functionality. However, a License Key is required to enable this feature in the agent software. Refer to the software user documentation for details on how to obtain a License Key.
- **Not Supported** — one or more units in the device list are not supported. Please ensure that you have downloaded and installed the latest service pack, if available, using Live Update. See "Live Update" on page 221 for more information.

*If the service pack release notes identify your device as being supported, but the device is still shown as unsupported in the Backup or Setup Wizard, then the current inventory file may be out of date. 3Com recommends that you refresh the inventory file and try again.*

*You can only apply a saved backup to a target device that has the same physical configuration as the source of the backup. The presence of a redundant module is recorded as part of the physical configuration stored in the backup file for a device. So for a device to have the same physical configuration, it must have the same redundant module too.*

*The Layer 3 module that is available for use with the Switch 1100 and Switch 3300 family of devices will not be configured by the Device Restore or Setup operations. The presence of these modules is recorded as part of the physical configuration stored in the backup file for a device, but the software configuration of the module is not saved.*

## Supported Device Parameters

The Device Backup operation saves the configuration of the agent software parameters summarized in Table 11:

**Table 11** Supported Parameters by Device Family

| Device Family | Supported Parameters |
|---|---|
| Switch 610/630<br>Switch 1100 Family<br>Switch 3300 Family | System Information; VLANs; Roving Analysis Port; Resilient Links; Port Trunks; Port Security; Spanning Tree; Port Configuration; Advanced Stack Setup; Users and User Access; RMon Alarms; RMon Events; Trap Destination; Network Interface Configuration; Serial Port Configuration |
| Switch 4300 | System Information; VLANs; Roving Analysis Port; Spanning Tree; Port Configuration; Port Priority; IGMP Setup; RMon Alarms; Trap Destinations |
| Switch 4400 Family<br>Switch 4005<br>Switch 4007/4007R<br>Wireless LAN Access Point 8000 | The agent software for these device families has native support for Backup and Restore. Please refer to the user documentation for these products for further details of the software parameters that are supported. |

*The following network interface settings are not applied to target devices by the Device Restore or Setup operations: IP address, subnet mask and default gateway.*

*User passwords and RADIUS secrets, where relevant, are not saved as part of the human readable backup files for security reasons. See* "Understanding Backup Files" *below for a list of device families whose configuration is stored in readable backup files.*

## Understanding Backup Files

Backup files are saved in a readable format called eXtensible Markup Language (XML). Every backup file is divided into two main sections, the *head* and the *body*. The head section describes the physical configuration of the device, at the time it was backed up. However, the content of the body section depends on the type of the source device. Table 12 shows how the content of the body section relates to the device family of the source device.

**Table 12** Backup File Content by Device Family

| Device Family | Content of Backup File (Body Section) |
|---|---|
| Switch 610/630<br>Switch 1100 Family<br>Switch 3300 Family<br>Switch 4300 | The entire software configuration of the device saved in a readable XML format. The software configuration can be applied to a device only using 3Com Network Administrator. |
| Switch 4400 Family | A reference to a single auxiliary file. The auxiliary file contains the software configuration of the device saved in a readable CLI command format. The auxiliary file can be restored to the device independently of 3Com Network Administrator, if desired, by using the device CLI or web interface. |
| Switch 4005<br>Switch 4007/4007R<br>Wireless LAN Access Point 8000 | A reference to one or more auxiliary files. The auxiliary files contain the software configuration of the device saved in an unreadable binary format. The auxiliary files can be restored to the device independently of 3Com Network Administrator, if desired, by using the device CLI or web interface. |

## Managing Backup Files

3Com Network Administrator saves all backup files to the following directory on your hard disk drive:

```
<INSTALL LOCATION>\backups
```

*The default install location of 3Com Network Administrator is:*

```
C:\Program Files\3Com\Network Administrator
```

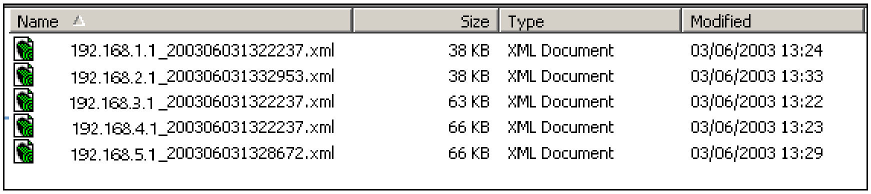
3Com Network Administrator does not delete backup files. Eventually, the list of backups for a device may become difficult to manage unless you manually delete unwanted backup files. To delete an unwanted backup file, locate the file in the backup directory on your hard disk using Window Explorer.

To locate a backup file you will need to know:

- The IP address of the source device at the time the backup was made.
- The date and time of the Device Backup operation that created the backup file

All backup files have the file extension `.xml`, and are named according to the scheme shown in Figure 64:

**Figure 64** Backup File Name Format



| Name | Size | Type | Modified |
|---|---|---|---|
| 192.168.1.1_200306031322237.xml | 38 KB | XML Document | 03/06/2003 13:24 |
| 192.168.2.1_200306031332953.xml | 38 KB | XML Document | 03/06/2003 13:33 |
| 192.168.3.1_200306031322237.xml | 63 KB | XML Document | 03/06/2003 13:22 |
| 192.168.4.1_200306031322237.xml | 66 KB | XML Document | 03/06/2003 13:23 |
| 192.168.5.1_200306031328672.xml | 66 KB | XML Document | 03/06/2003 13:29 |

*When deleting unwanted backup files you should take care to also delete any auxiliary files referenced by the backup in order to conserve hard disk space. Auxiliary files to a backup have the same filename as the backup file but a different extension (e.g.* `bak`*,* `unit1`*,* `module*`*)*

## Key Considerations

The following section provides assistance when using Backup, Restore and Setup.

### How Backup Files are Discarded

Before the Device Backup operation saves a backup for a device, it performs a consistency check. The consistency check looks for any existing backups that conflict either with the physical identification or the physical configuration of the current device. Any existing backups that fail this consistency check will be discarded before a new backup is saved. This happens if:

- There are existing backups associated with the physical identification of the current device but the physical configuration stored in the existing backups does not match the physical configuration of the current device.

- There are no existing backups associated with the physical identification of the current device but there are existing backups associated with two or more other physical identifications that partially match the physical identification of the current device. This can happen if you combine units from two or more existing devices to form a new device.

Backup files that are discarded are not deleted from your hard disk but are moved to the following directory:

```
<INSTALL LOCATION>\backups\lost
```

*The default install location of 3Com Network Administrator is:*
`C:\Program Files\3Com\Network Administrator`

## Potential Hazards when using Restore and Setup

The Device Restore and Setup operations initialize most types of device prior to applying the software configuration. The initialization of a device that is connected to your network can cause network loops. It is particularly likely that a network loop will occur if the target devices are configured with any of the following features prior to the start of the operation:

- VLANs
- Spanning Tree
- Aggregated Links
- Resilient Links

3Com strongly recommends that you isolate target devices from the rest of the network and connect them directly to the management station before using Restore or Setup.

## Why Errors can Occur during Restore and Setup

A common reason for the failure of a Device Restore or Setup operation is a loss of contact with the target device. This can occur either when the device is initialized prior to configuration or while the device is being configured. If this happens, please ensure that the target device is either connected directly to the management station or is connected to the management station through a simple unmanaged hub or switch.

If the restored configuration you are applying results in ports being disabled, you will also need to ensure that the device is connected to the management station through a port that does not become disabled when the configuration is applied.

# 7 Agent Update

## Overview

This chapter describes how 3Com Network Administrator can be used to manage the agent software on 3Com devices across your network and to ensure that the 3Com devices on your network are running the latest agent software available to you.

You can use the Agent Update feature to:

- Upgrade all supported 3Com devices on your network to the latest agent software you have available.
- Find 3Com devices on your network that are running out-of-date agent software.
- Import agent software from files on disk that may have been downloaded from 3Com.
- Upgrade or downgrade the agent software on individual 3Com devices.

This chapter covers the following topics:

- Key Concepts
- Components
- Examples
- Useful Information and References
- Key Considerations

## Key Concepts

This section describes the key concepts associated with the Agent Update feature.

### Agent Image Files

You can use the Agent Update Wizard to import agents that you have obtained from elsewhere, for example downloaded from the web. This allows you to import older agents, to create a comprehensive database of agent versions.

Some agent files can be applied to more than one specific type of device or to any type of device within a particular device family.

### The Internal TFTP Server

3Com Network Administrator contains a built in TFTP server that is started when you begin an Agent Update operation. The server is responsible for transferring agent software to each device when the device requests an agent image file. The Agent Update operation stops the internal TFTP Server once the operation has completed.

TFTP is an insecure file transfer protocol that requires no username or password. Therefore, 3Com Network Administrator places restrictions on any requests in order to prevent any unauthorized TFTP activity. The internal TFTP Server incorporates the following safeguards:

- TFTP requests are accepted only from the IP address of the devices included in the current Agent Update operation.
- Only requests for file downloads are permitted.
- The TFTP server only runs for the duration of an Agent Update operation.

### Scheduling

You can schedule an Agent Update operation to be carried out when the network is at its least active and will cause the least disruption to you on the network. Scheduling requires the application to be running when the operation is due to take place. It is dependant on the system clock, so in order for a scheduled agent update to run at the correct time, the system clock must be accurate.

## Components

The following section describes the principles of updating agents using 3Com Network Administrator.

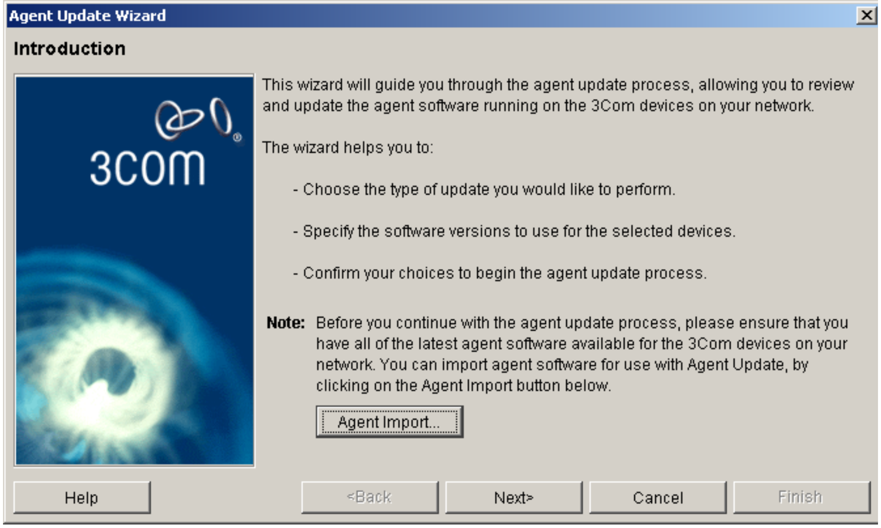
## Agent Update Wizard

The Agent Update Wizard guides you through the process of upgrading devices in the network. This section describes the function of each step or dialog used in the wizard.

### Introduction Step

The *Introduction* step in the Agent Update Wizard outlines the agent update process, summarizing the choices covered by the wizard as shown in Figure 65. This step also allows you to import a new agent that may have been downloaded from the 3Com website or provided on a product CD. To import an agent, click *Agent Import...* to launch the *Agent Import* dialog. This dialog lets you select an agent image file to import.

**Figure 65** Agent Update Wizard - Introduction



Agent Update Wizard

Introduction

This wizard will guide you through the agent update process, allowing you to review and update the agent software running on the 3Com devices on your network.

The wizard helps you to:

- Choose the type of update you would like to perform.
- Specify the software versions to use for the selected devices.
- Confirm your choices to begin the agent update process.

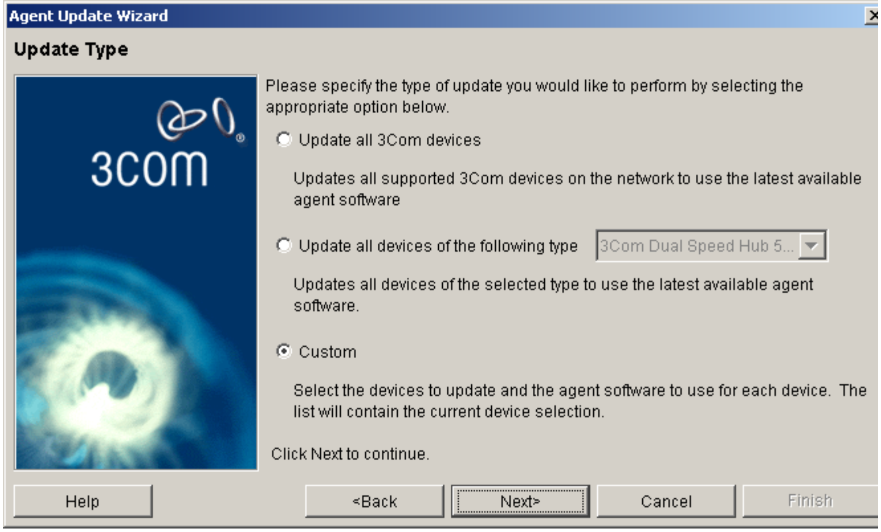
**Note:** Before you continue with the agent update process, please ensure that you have all of the latest agent software available for the 3Com devices on your network. You can import agent software for use with Agent Update, by clicking on the Agent Import button below.

*Importing agents this way only allows the agent image to be imported; any release notes associated with the agent will be ignored.*

## Update Type Step

The *Update Type* step of the wizard offers you three options as shown in Figure 66.

**Figure 66** Agent Update Wizard - Update Type



Update Type

Please specify the type of update you would like to perform by selecting the appropriate option below.

○ Update all 3Com devices

Updates all supported 3Com devices on the network to use the latest available agent software

○ Update all devices of the following type [3Com Dual Speed Hub 5...]

Updates all devices of the selected type to use the latest available agent software.

● Custom

Select the devices to update and the agent software to use for each device. The list will contain the current device selection.

Click Next to continue.

Each option determines the type of update being performed. The options are:

- **Update all 3Com devices** — updates all devices in the network that meet the following criteria:
  - Supported by Agent Update
  - Not running the latest version of available agent software already

  If this option is selected you can schedule when to perform the operation (by selecting *Next* from the *Update Type* dialog). See "Scheduling Step" on page 140 for further information.

- **Update all devices of the following type** — updates all devices that match the device type selected from the drop down list shown.

  For example, selecting a Switch 4900 will match the 4900, the 4900 SX, 4924 and 4950 units.

*Even though the Switch 1100s and 3300s share the same agent, they are listed separately in the* Update by type to latest *list box. The Switch 610s and 630s are not listed separately, but will appear when you select all by type for 1100 and 3300 respectively. 3Com Network Administrator does not distinguish between the 610/1100 and 630/3300.*

- **Custom** — allows full control over the Agent Update operation. You can specify each device to update, and for each device, the particular agent version to update to. You can also import agents for any device using a similar mechanism to that used in the *Introduction* step.

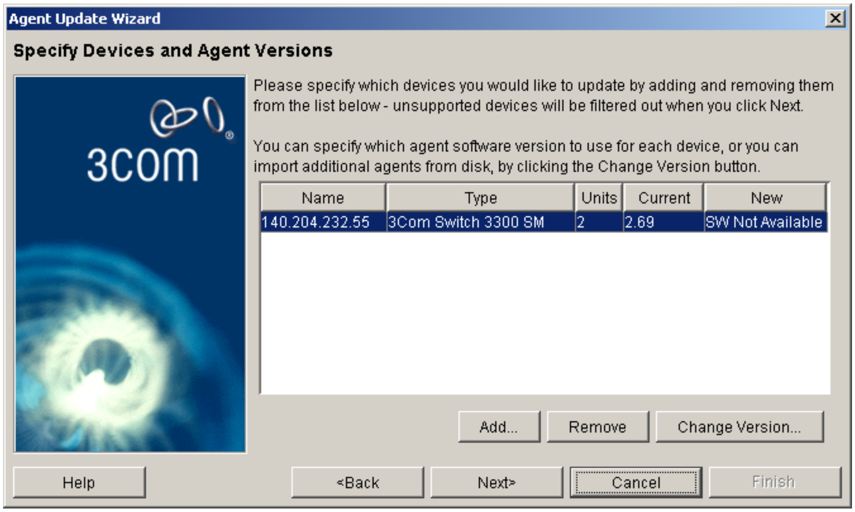
  This option is the default if any devices were selected when launching the wizard. If *Next* is selected with this option chosen, the *Specify Devices and Agent Versions* step will display listing the devices that are selected.

Some or all of the following steps now display depending on the option you selected in the *Update Type* step.

### Specify Devices and Agent Versions Step

In this wizard step, you can specify the devices that should be upgraded during this operation and choose which agent version to upgrade to from a list of available versions as shown in Figure 67.

**Figure 67** Agent Update Wizard - Specify Devices and Agent Versions



Agent Update Wizard

Specify Devices and Agent Versions

Please specify which devices you would like to update by adding and removing them from the list below - unsupported devices will be filtered out when you click Next.

You can specify which agent software version to use for each device, or you can import additional agents from disk, by clicking the Change Version button.

| Name | Type | Units | Current | New |
|---|---|---|---|---|
| 140.204.232.55 | 3Com Switch 3300 SM | 2 | 2.69 | SW Not Available |

The table lists any devices that you have chosen for the Agent Update operation. If any devices were selected from the device list prior to launching the Agent Update wizard, these will be present in this list by default.

To add devices to the table, click *Add* to display the *Find Device* dialog which enables you to search the application for any device. Click *Remove* to remove the selected device(s) from the list.

To select other agent versions to upgrade to, click *Change Version* to launch the *Change Agent Version* dialog, which offers a list of available agent versions for the selected device.

The device table contains the following information about each device:

- **Name** — specifies the name or IP address of the 3Com device.
- **Type** — specifies the 3Com family name of the listed device.
- **Units** — specifies the number of units in a stack or distributed fabric.
- **Current** — specifies the current version of agent software running on the device.

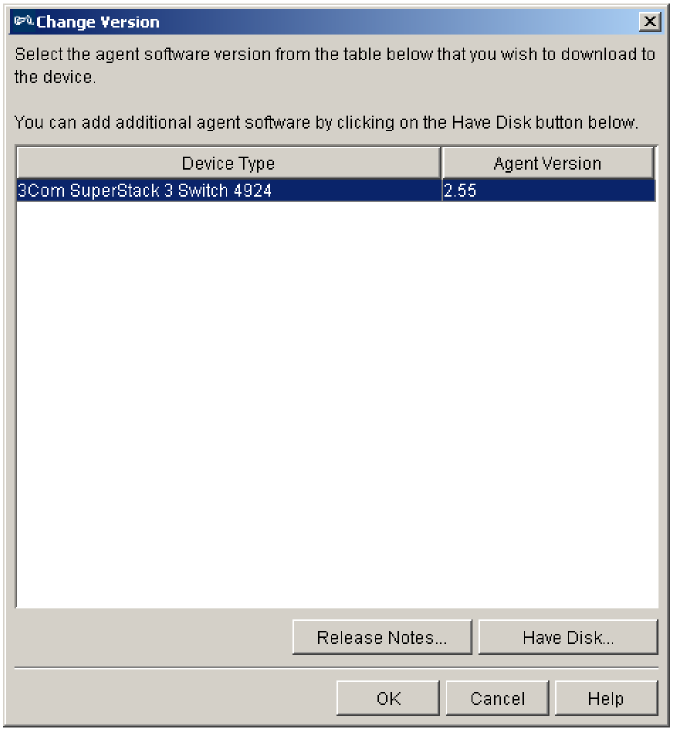
  The *Current* column displays a comma-separated list of versions if the device has multiple units or modules that are currently running different agent software versions.
- **New** — specifies the latest version of the agent software available for that device type. If you proceed, this is the version of agent to which the device will be updated.

  The *New* column displays the agent version the device is to be updated to unless the agent is not available or not supported, indicated by one of the following labels:
- **SW Not Available** — displays if a device is selected that is supported by Agent Update, but has no suitable agent software available.
- **Not Supported** — displays if Agent Update does not support the device. See "Supported Devices" on page 148 for more information on devices that are supported by Agent Update.

### Change Agent Version Step

Click *Change Version* on the *Specify Devices and Agent Versions* wizard step to launch the dialog shown in Figure 68. The dialog will list all agent versions that Agent Update has imported for the selected device using the Agent Import tool.

**Figure 68** Agent Update Wizard - Change Version



Select the agent software version from the table below that you wish to download to the device.

You can add additional agent software by clicking on the Have Disk button below.

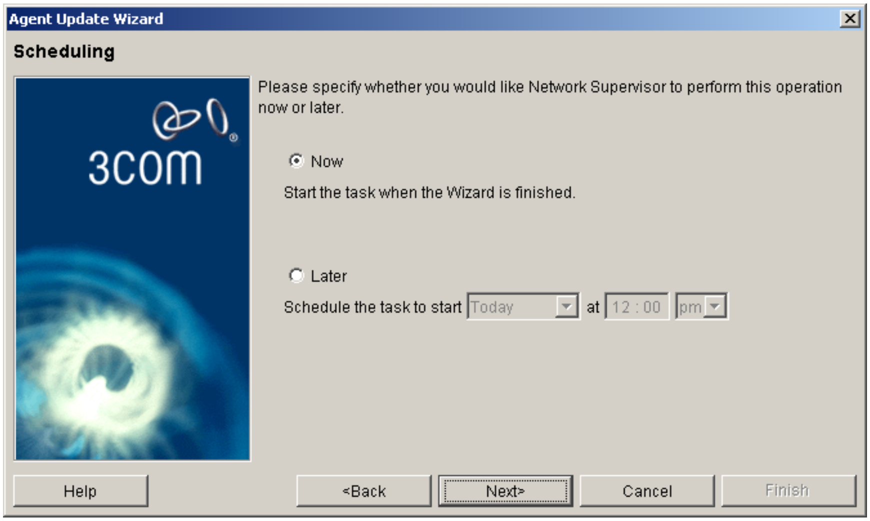
| Device Type | Agent Version |
|---|---|
| 3Com SuperStack 3 Switch 4924 | 2.55 |

To add a new version to the list, click *Have Disk*, which will launch an *Add Agent File* dialog. This lets you specify an agent image file to use. If the file selected is a valid agent file, it will be added to the agent version database and if it is applicable to the currently selected device on the Agent Update Wizard, it will be added to the list.

## Scheduling Step

You can specify a time to carry out the operation. The default option in this step is *Now* which will perform the Agent Update operation as soon as the wizard has finished as shown in Figure 69.

**Figure 69** Agent Update Wizard - Scheduling



Agent Update Wizard

Scheduling

Please specify whether you would like Network Supervisor to perform this operation now or later.

● Now

Start the task when the Wizard is finished.

○ Later

Schedule the task to start Today at 12 : 00 pm

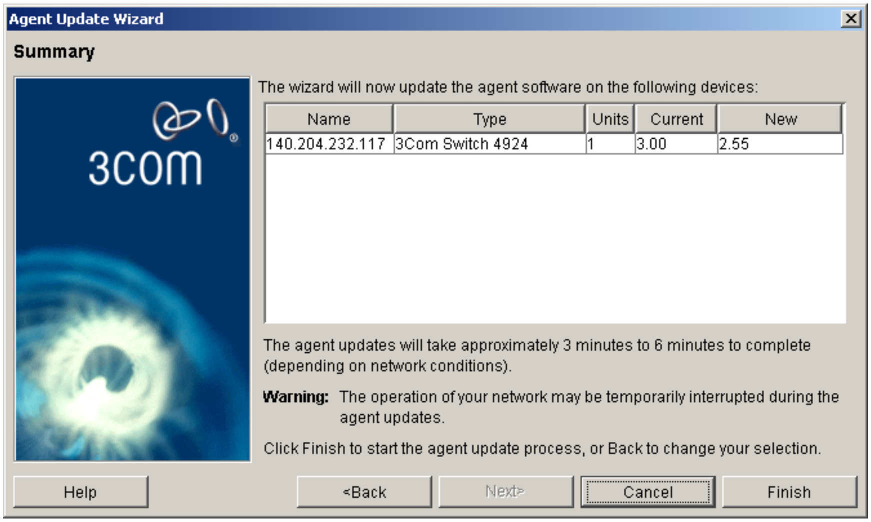
If *Later* is selected, the time selection is enabled and you can choose any time in the next week to schedule the operation. The time field is in 12-hour format so remember to set to am/pm.

Once an Agent Update operation has been scheduled, the basic details for the operation can be seen in the *Scheduled Tasks* dialog (*Tools > Scheduled Tasks*). To cancel the operation select the operation from the table of scheduled tasks and click *Remove*.

## Summary Step

The *Summary* step presents you with the choices made during the wizard as shown in Figure 70:

**Figure 70** Agent Update Wizard - Summary



Agent Update Wizard

Summary

The wizard will now update the agent software on the following devices:

| Name | Type | Units | Current | New |
|---|---|---|---|---|
| 140.204.232.117 | 3Com Switch 4924 | 1 | 3.00 | 2.55 |

The agent updates will take approximately 3 minutes to 6 minutes to complete (depending on network conditions).

**Warning:** The operation of your network may be temporarily interrupted during the agent updates.

Click Finish to start the agent update process, or Back to change your selection.

The table contains a row for each device that Agent Update will attempt to upgrade should you proceed. This list will depend on the choices you made through the wizard. For example, if the *Update all devices of the following type* option is selected on the *Update Type* step, then the list will contain all devices and variants of the selected type that were found in the inventory. If the Custom option was selected, the list should contain those devices selected on the *Specify Devices and Agent Versions* step.

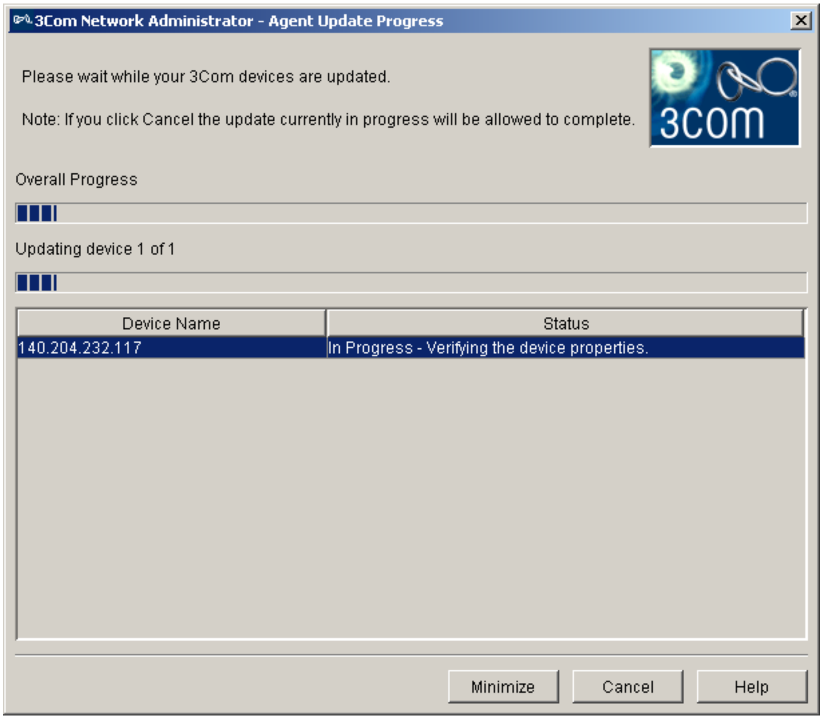
Devices can also be removed from the list by 3Com Network Administrator for the following reasons:

- The device is not supported — any unsupported devices are removed.
- Downgrading the device is not allowed — if the list contains devices that cannot be downgraded for any reason, and a downgrade was selected for the device, the operation is blocked.

### The Progress Dialog

The *Progress* dialog displays when an Agent Update operation is due to start. It displays the list of the devices to be upgraded and the status of each update as it progresses as shown in Figure 71:

**Figure 71** Agent Update Wizard - Progress Dialog



3Com Network Administrator - Agent Update Progress

Please wait while your 3Com devices are updated.

Note: If you click Cancel the update currently in progress will be allowed to complete.

Overall Progress

Updating device 1 of 1

| Device Name | Status |
|---|---|
| 140.204.232.117 | In Progress - Verifying the device properties. |

The updates are performed one at a time, with the lower of the two progress bars showing the progress of the current device and the top progress bar showing the progress of the entire operation. The list of devices shows the current status of each device as it updates. There are five main stages of each update. These are:

- Preparing the device
- Verifying the device properties
- Contacting the device
- Loading the agent software to unit x of y
- Verifying the update

During the verifying device properties stage, Agent Update will examine the properties of the device to ensure that it is the expected device. If the device is not what Agent Update was expecting, then the update for that device is skipped.

To verify that a download was successful, Agent Update will read the device details at the end of the update and check that the new software version has successfully changed.

## Agent Update Events

An HP OpenView alarm is generated in HP OpenView for each device that 3Com Network Administrator attempts to update as part of the Agent Update operation.The alarm source is the IP address of the device and both the severity of the alarm and the alarm message indicate whether the attempt to update the agent was successful. The detail of the message for a successfully updated device includes the previous agent version and the new agent version that is running on the device. For devices that could not be updated, the detail of the alarm message describes what went wrong and suggests possible resolutions to the problem.

## Agent Update Reports

The following reports are produced by Agent Update.

### Agent Update Summary Report

When an Agent Update operation completes, the Agent Update Summary report is automatically generated. You can choose to view the report from the *Agent Update Summary* dialog shown at the end of the operation.

The Agent Update Summary report provides the following information:

- A list of the devices that have been successfully updated by the operation. The previous and new versions are shown for each device.
- A list of the devices that could not be updated by the operation. The current and required agent versions are shown for each device. 3Com Network Administrator will also report a reason for the failure and suggest possible resolutions.

### Agent Audit Report

You can use the Agent Audit report to determine which of the devices on your network are running the latest available agent software, and which devices are running out-of-date software.

*You can generate an Agent Audit report at any time from the* Generate Reports *tab of the* Reports *dialog, launched from* Tools > Reports*.*

The Agent Audit report provides the following information:

- A list of the 3Com devices on your network that are running the latest agent release available for them.
- A list of the 3Com devices on your network that are running up-to-date agent software.
- A list of the 3Com devices on your network that are not supported by Agent Update.
- A list of the 3Com devices on your network for which there are no supported agent versions available locally.

## Examples

The following section details some useful examples of how to use Agent Update.

### Update all Switch 4400's with a New Agent

You have a new agent release for the Switch 4400. You want to update all Switch 4400 devices on the network to the new agent version this evening. To do this:

1. Select *Agent Import* from the *Device* > *Agent Import* menu.
2. In the *Agent Import* dialog, locate the agent image.

   Agents for the Switch 4400 fit the naming convention `s3mXX_YY.bin` and are sometimes found as self-extracting executable files with the format `s3mXX.YY.exe`. Select the binary `.bin` file.

3. Launch the Agent Update Wizard from the *Device* > *Agent Update* menu.
4. Click *Next* on the *Introduction* step to display the *Update Type* step. Click the *Update all devices of following type* radio button and click *3Com Switch 4400* from the drop-down menu.
5. Click *Next* to display the *Schedule* step, then select the *Later* radio button to enable the time selection. Enter *11.00pm* to avoid disrupting the use of the network during working hours.

**6** Click *Next* to display the *Summary* step and check that the details are all correct before clicking *Finish* to start the operation.

**7** View the scheduled tasks list to ensure the new task is present by clicking *Tools* > *Scheduled Tasks*.

**8** Leave the application running and next morning, check that there is a *Summary* dialog indicating that the Agent Update operation was successful.

**9** Leave the *View report* check box checked and click *OK* to view the report. Once it appears, check that all entries in the report indicate that all of the Switch 4400s were successfully upgraded to the new agent version.

### Detecting and Downgrading a Problem Device

There is a problem device on the network. You want to see if anything has changed recently and, if so, undo the changes. To do this:

**1** Launch the *Reports* dialog by selecting the *Tools* > *Reports* menu.

**2** From the *Report Types* list box, select the *Device History* report and then click *Generate Report* to generate and launch the report.

**3** You read the report and notice that the device in question was recently upgraded to a beta version.

**4** Return to the application, select the device and launch the Agent Update Wizard from the *Tools* > *Agent Update* menu.

**5** Click *Next* to accept the default choices in the wizard.

**6** Check that the selected device is in the list by default and that the *Current* version is the beta version seen in the Device History report and the *New* version is the latest available release version.

**7** Click *Next* to display the *Summary* step and click *Finish* to start the downgrade of the device.

## Useful Information and References

The following section provides assistance when using Agent Update on your network.

### Supported Devices

Some types of devices are supported only from a minimum agent version onwards. If you want to upgrade the agent of a device that is currently running an unsupported agent version, you must use another means to upgrade the agent for the first time.

*The supported devices are listed in Appendix A on page 241.*

### Agent Image Filenames

3Com agent image files follow a naming convention that helps you to identify the device family that the agent can be applied to.

*Some types of device will reject attempts to update them using agent files that do not follow the naming scheme. For this reason, 3Com recommends that you do not rename your agent files.*

Table 13 shows the agent filename format for the device families supported by Agent Update.

**Table 13** Agent Filename Format by Device Type

| Device Family | Agent Filename Format |
|---|---|
| PS Hub 40 | `psfXX_xx.bin` |
| PS Hub 50 | `pshXX_xx.bin` |
| Dual Speed Hub 500 | `dshXX_xx.bin` |
| Switch 610/630/1100/3300 | `s2sXX_xx.bin` |
| Switch 4200 series | `S42XX_xx.bin` |
| Switch 4300 | `s43XX_xx.bin` |
| Switch 4400 | `s2mXX_xx.bin` |
| Switch 4900 series | `s3gXX_xx.bin` |
| Switch 4050/Switch 4060 | `gmiXX_xx.bin` |
| Switch 4005 | `4005vXxx.bix` |

| Device Family | Agent Filename Format |
|---|---|
| Wireless LAN Access Point 8000 | `opXXxxxx.bin` (operational code)<br>`fsXXxxxx.bin` (file system)<br>`fsXXxxxx.bin` (combined operational code and file system) |
| Webcache series | `s3b_XX_xx.bin` |

*'XX' represents the major version number and 'xx' the minor version number of the agent software contained in the file.*

## Key Considerations

The following section provides useful information and advice on updating agents.

### Co-existence With Other TFTP Servers

3Com Network Administrator cannot perform Agent Update operations whilst another TFTP server is in use on the same machine. If an Agent Update operation fails due to a conflict with another TFTP server, you will be informed of this in the Agent Update Summary report. You must stop the other TFTP server before the Agent Update operation can take place.

### Considerations When Downgrading Devices

You should always read the agent software release note before downgrading a device, since not all agent software can be overwritten with significantly older software.

### Troubleshooting Device Problems Following Agent Update

If you find that your device is no longer responding following an attempt to update the agent, the problem could be caused by one of the following conditions:

- There are network problems preventing you from contacting the device.
- The device has not yet returned to an operational state following the completion of an update.
- The device IP settings have been changed or cleared.
- An interruption in the TFTP transfer of the agent file has left the device in a non-operational state.

3Com recommends that you use your usual network monitoring tools to check that there are no general problems with your network before trying to troubleshoot problems with the device.

Once you are certain that the device is not responding you should physically inspect the device to ensure that all units or modules are operational. It can take several minutes for all of the units or modules in a device to return to an operational state following an update of the agent software. Therefore:

- If the device appears to be in an operational state, try to log in to the device using a connection to the console port and check that the device has appropriate network interface settings.
- If the device appears to be in a non-operational state, then it could be that the transfer of the agent file to the device during the Agent Update operation was interrupted. In this case, most 3Com devices will try to download the agent image from your management station indefinitely. However, 3Com Network Administrator will not accept TFTP requests once the Agent Update operation has completed.

  To recover from this situation you can either use the serial update utility as detailed in the release notes for your device or you can run a standalone TFTP server on your management station that will service the device requests.

## Repeated Timeouts

If your attempts to upgrade a device repeatedly fail and the Agent Update Summary report indicates that the failure is due to a device timeout or 'TFTP not reachable' error, then you may need to increase the timeout and retry values for the 3Com Network Administrator internal TFTP server.

You can alter the timeout and retry values for the internal TFTP server by editing the following file:

```
<INSTALL LOCATION>\ext\com\coms\wsd\tnsext\agentupdate\
AUProperties.XML
```

*The default location of 3Com Network Administrator is:*
`C:\Program Files\3Com\Network Administrator`

*3Com recommends that you alter the timeout and retry values in small increments, since large changes to these values can result in adverse performance of the Agent Update operation.*

To alter the time-out and retry values:

**1** Close down 3Com Network Administrator.

**2** Open the `AUProperties.XML` file using Notepad or another text editor.

**3** Look for an integer value surrounded by the following tags:

```
<TIMEOUT>,</TIMEOUT>
```

This value controls the timeout, in seconds, for TFTP packets sent by the internal TFTP server. Increment the value to increase the TFTP timeout.

**4** Look for an integer value surrounded by the following tags:

```
<RETRIES>,</RETRIES>
```

This value controls the number of times a single TFTP packet transmission is retried by the internal TFTP server. Increment the value to increase the number of TFTP retries.

**5** Restart 3Com Network Administrator and try to update the problem device again.

# 8 PRIORITIZING NETWORK TRAFFIC

## Overview

This chapter describes how 3Com Network Administrator can be used to prioritize network traffic on the 3Com devices on your network.

By enabling prioritization, you can specify the importance of certain types of network traffic (such as traffic to and from database servers or NBX phone traffic) over others. This can ensure that important traffic on a configured device flows quicker than other traffic and is less likely to be dropped in times of congestion.

Prioritizing network traffic also enables you to ban certain types of network traffic (such as games traffic or connections to streaming media servers). This is called **blocking**. If a configured device sees traffic that has been blocked, the blocked traffic is prevented from being transmitted over your network.

The following topics are covered in this chapter:

- Key Concepts
- Components
- Examples
- Useful Information and References
- Key Considerations

## Key Concepts

Traffic prioritization has three basic aims:

- To ensure that traffic defined as being more important flows through the network quicker than other types of traffic.
- To ensure that important traffic is less likely to be dropped if there is congestion on the network.
- To prevent traffic that has been blocked from flowing on the network.

In order to achieve the aims of traffic prioritization across the network, each Switch in the network must provide facilities for:

- Performing identification of the most important traffic and traffic that should be blocked. This is known as **classification**.
- Performing suitable **actions** as a result of classification to meet the needs of the particular traffic type that classification identified. There are three actions that can be performed; **marking**, **queuing** and **dropping**.

### Classification

Classification identifies different types of traffic by examining the contents of a packet or set of packets. For example, a packet received by a device can be identified as traffic to and from your database server if the destination or source IP address in the packet matches the IP address of the database server.

There are many fields in a packet that a device may use to classify traffic, including:

- Ethernet type
- Source or destination MAC address
- IP protocol
- Source or destination TCP port
- Source or destination UDP port

Classification can also be much more complex than simply examining a field in a packet. It can involve examining multiple fields in a packet parsing and analyzing the contents of a packet or even analyzing flows of traffic rather than a single packet.

Classification is configured on a device as a set of rules. Each rule defines a particular way of identifying the type of traffic. For example, a rule may state that SNMP traffic can be identified as UDP packets that have either the source or the destination UDP port set to the value 161.

## Marking

Due to the numerous possibilities for classifying packets, not every device can classify the same packets in the same manner. Some devices are capable of extremely complex classification (*complex classification devices*), while other devices may only be able to match traffic based on the content of one or two fields (*simple classification devices*). For example, this can mean that while one device in your network is able to identify traffic to and from your database server using the destination or source IP address in the packets, another device may not be able to.

There are two standards that specify how a complex classification device can modify packets in a straightforward manner so that a simple classification device can still identify how important those packets are.

This modification of packets is known as marking and the two standards are:

**IEEE 802.1D** — defines an extended MAC header (known as a tagged header) which contains a user priority field (known as the 802.1p tag), which takes one of eight values (0 - 7) to represent the priority of the packet.

**IETF RFC 2474** — defines the use of the Differentiated Services (DiffServ) field in the IP header. This field can take one of sixty-four values (0 - 63) which are known as DiffServ codepoints (or DSCPs) to represent the *quality of service* requirements of the packet. There are no restrictions on what a particular codepoint value may mean, however one use could be to simply represent the priority of the packet.

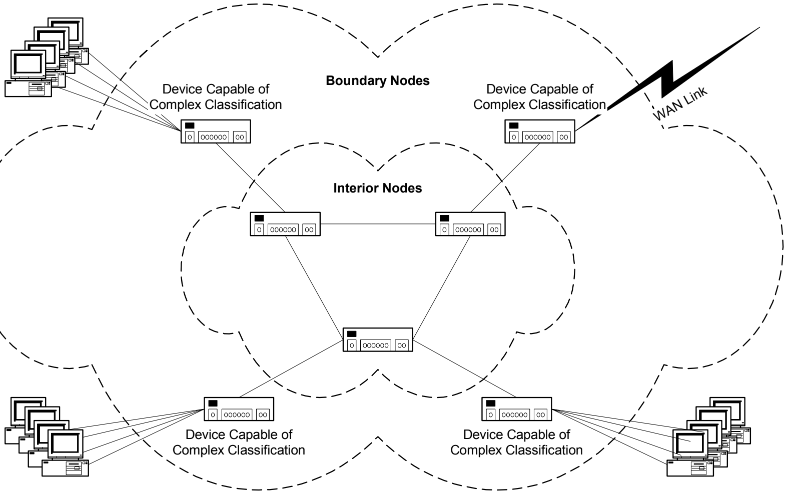
*More information on these standards is available in "User Priority Field" on page 180 and "DiffServ Codepoint Field" on page 181.*

As these standards each define a single field in which to store the marking, it means that simple classification devices can still be used as part of a network-wide traffic prioritization solution provided that the following conditions are met:

- Simple classification devices must be able to classify on the user priority field, the DiffServ field or both.
- Complex classification devices must be able to mark packets appropriately based upon their traffic type. This must be done using a marking mechanism that the simple classification devices are able to classify. Whilst it is possible to use different marking schemes at different locations in the network 3Com recommends that, if possible, one is selected and used throughout the network.
- Packets sent across the network must first pass through a complex classification device (such as a 3Com SuperStack 3 Switch 4400) so that they can be marked appropriately. This enables simple classification devices to prioritize packets.

For traffic prioritization to work on an end-to-end basis in your network it is recommended that you structure your network as shown in Figure 72.

**Figure 72** Network Topology


Boundary Nodes
Device Capable of Complex Classification
Device Capable of Complex Classification
WAN Link
Interior Nodes
Device Capable of Complex Classification
Device Capable of Complex Classification

The boundary nodes (shown in the Topology example) are complex classification devices and can perform the appropriate marking of packets. This means that any interior nodes that are simple classification devices are still able to determine the correct traffic prioritization to perform.

## Queuing

The first two aims of traffic prioritization (forwarding important traffic through the device faster than other traffic and reducing the risk of dropping important traffic) are provided by the queuing mechanism as follows:

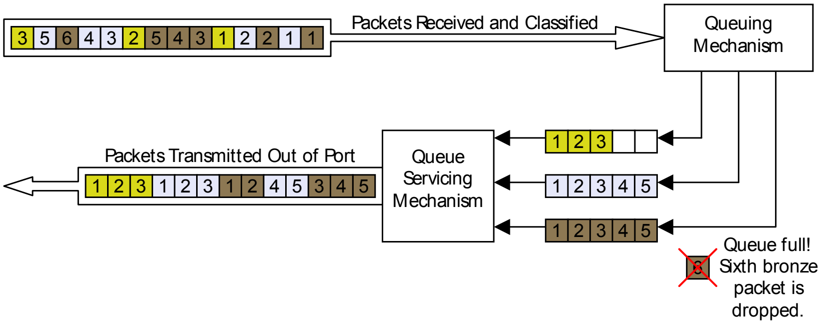
1. The classified traffic is queued for output on a particular port in multiple queues rather than in a single queue (as performed on devices that are not capable of traffic prioritization) and those queues are serviced in a particular way that favors the more important traffic over other traffic.
2. Each of the queues is shared between one or more different types of traffic that have been defined as having a similar level of importance.
3. If a particular queue fills up with packets then any further packets for that queue will be dropped until the queue is serviced. This will clear some of the packets from the queue.
4. Packets are taken off the queues and transmitted out of the port according to the particular queue servicing mechanism that is in place. A device may support one or more of the various queue servicing mechanisms that are available, which include weighted round robin and strict priority queueing. Each of these queuing mechanisms has its own characteristics yet they are all aimed at ensuring higher priority traffic is processed and forwarded by the device quicker than other traffic.

An example of the results of a queuing servicing mechanism is illustrated in Figure 73. It shows how important traffic flows through the network quicker than the less important traffic and reduces the likelihood of the more important traffic being dropped. The device in the figure defines traffic as being gold, silver or bronze (gold being the most important) with a queue for each type of traffic.

The example illustrates what happens when a device receives a set of packets of different types that are destined for the same port:

- The queuing mechanism takes the packets (which are received in no particular order) and, based upon whether they were classified as gold, silver or bronze, places them in the gold, silver or bronze queue. The bronze queue does not have enough space to hold all of the bronze packets and so the sixth bronze packet is dropped.
- The queue servicing mechanism takes packets off the queues, according to the particular mechanism in use and the way it is configured, and transmits them out of the port. This effectively re-orders the packets. The gold packets are transmitted before all other packets whilst the silver packets are transmitted in preference to the bronze ones. In the particular queue servicing mechanism used here it does not immediately transmit all of the silver packets after the gold, instead it allows some bronze packets to be transmitted so that even the lowest priority traffic can receive some amount of bandwidth.

**Figure 73** Queue Servicing Mechanism



3 5 6 4 3 2 5 4 3 1 2 2 1 1
Packets Received and Classified
Queuing Mechanism
1 2 3
1 2 3 4 5
1 2 3 4 5
Packets Transmitted Out of Port
1 2 3 1 2 3 1 2 4 5 3 4 5
Queue Servicing Mechanism
6
Queue full! Sixth bronze packet is dropped.

If these queuing operations are performed on all devices in the network then the overall effect is to speed up the flow of important traffic through the entire network. Also, by processing the queues containing more important traffic more frequently this reduces the likelihood that the queue will fill up because the queue will be emptied quicker and therefore reduce the risk that the more important traffic will get dropped.

## Dropping

The action of dropping allows the device to prevent blocked traffic from flowing on the network. This is achieved by discarding (dropping) packets that are identified via classification as traffic that should be blocked.

## Service Levels

The overall set of actions that are performed as a result of a particular classification are commonly known as a service level. Service levels enable a device configuration to be specified in terms of a mapping between the classification rules and the service levels. This enables several classification rules to share the same service level.

For example, a device may be configured with service levels for:

- Business critical traffic
- Voice traffic
- The CEO's traffic
- Blocked traffic
- All other traffic

Each of these service levels could perform different queuing and marking of the packets assigned to them.The service level for blocked traffic would not need to perform queuing or marking as traffic assigned to it would be dropped. The device can then be configured with a set of classification rules which are mapped to the service levels as shown in Table 14.

**Table 14** Service Levels

| **Classification Rules** | **Service Level** |
|---|---|
| Traffic to or from the database server | Business Critical Service Level |
| Traffic to or from the email server | Business Critical Service Level |
| Traffic to or from the company website | Business Critical Service Level |
| Phone traffic | Voice Service Level |
| Traffic to or from the CEO's PC | CEO's Service Level |
| Game traffic | Blocked Service Level |
| All other traffic | All Other Traffic Service Level |

Service levels enable easy identification of end-to-end treatment of traffic. If the example was to be configured appropriately on the devices throughout the network, it would be possible to say that database traffic is treated as business critical throughout the network.

Settings within a service level may vary from device to device depending upon the device's capabilities. One device, for example, may have four queues whilst another device may have two. As a result, a particular service level on one device may put the traffic in queue 3 while on another device it may be queue 1. However, identifying the service levels by name simplifies the understanding of the configuration.

## Configuring the Network for End-to-end Traffic Prioritization

When some devices in a network are complex classification devices and other devices are simple classification devices, it is necessary to apply configurations in such a way that the markings applied by the complex classification devices are treated appropriately by the simple classification devices.

In the previous example it was possible to specify that each service level marked its traffic with a DiffServ codepoint, assuming that the device in question was a complex classification device. The DiffServ codepoints can be seen in Table 15.

**Table 15** DiffServ Codepoints

| Service Level | DiffServ Codepoint |
|---|---|
| Business Critical Service Level | 16 |
| CEO's Service Level | 24 |
| Voice Service Level | 46 |
| All Other Traffic Service Level | 0 |

*The DiffServ codepoints chosen in the table above are taken from the recommended values from RFC2474 and RFC3246.*

*The Blocked Service Level does not require a DiffServ codepoint value as the traffic is dropped anyway which makes marking the traffic unnecessary.*

In order for devices to be able to provide suitable prioritization when they are not capable of identifying the types of traffic, it is possible to configure the devices to identify the traffic by their DiffServ codepoint.

These devices would be configured with mappings between classification rules and service levels as shown in Table 16:

**Table 16** DiffServ Codepoints and Service Levels

| Classification Rule | Service Level |
|---|---|
| Traffic marked with DiffServ codepoint 16 | Business Critical Service Level |
| Traffic marked with DiffServ codepoint 24 | CEO’s Service Level |
| Traffic marked with DiffServ codepoint 46 | Voice Service Level |
| Traffic marked with DiffServ codepoint 0 | All Other Traffic Service Level |

When these devices receive packets they can simply examine the DiffServ codepoint field of the packets to determine the service level, rather than performing the more complex analysis that they are incapable of.

## Components

The following section describes the principles of traffic prioritization using 3Com Network Administrator.

### Prioritize Network Traffic Wizard

The Prioritize Network Traffic Wizard enables you to simplify traffic prioritization configuration on your network without the need to manually set up classifiers, dropping, queuing and marking.

*The Prioritize Network Traffic Wizard is launched from* Tools > Prioritize Network Traffic.

The wizard allows you to select:

- Servers that traffic should be prioritized to and from.
- Servers whose traffic (transmitted or received) should be blocked on your network.
- Applications whose traffic you would like to prioritize.
- Applications whose traffic should be blocked on your network.

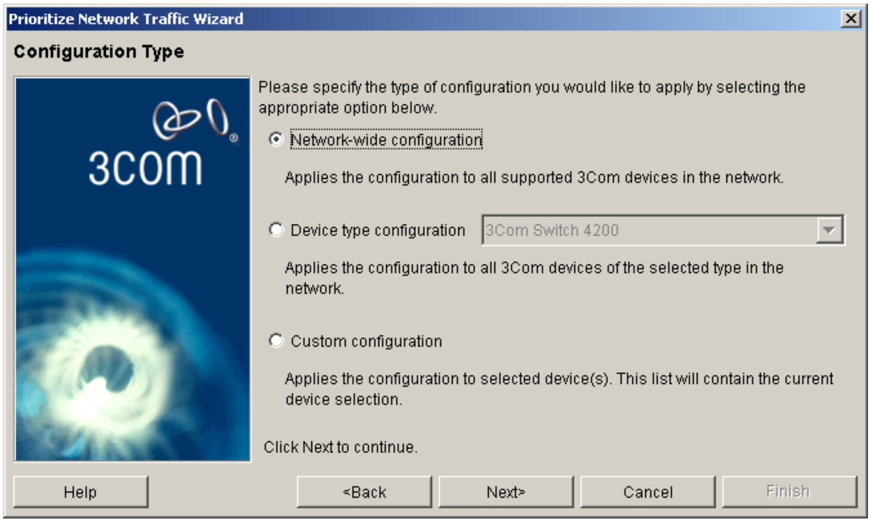
The wizard determines which of the devices it configures are capable of the required classification and handles these devices as boundary nodes. These devices are configured by the wizard to classify the traffic and to apply appropriate DiffServ codepoint markings. Devices not capable of the required classification are configured by the wizard to classify traffic based upon the DiffServ codepoint values that the boundary nodes mark the traffic with. This ensures that all configured devices are able to participate in the prioritization of network traffic.

*Whilst the Prioritize Network Traffic Wizard configures devices to mark the user priority field as well as the DiffServ codepoint, it does not configure devices to use the tagged MAC headers. However, if VLANs have been configured on some or all of the ports on the configured devices then the appropriate user priority data will be added to the packets that are transmitted out of these ports.*

## Configuration Type Step

You can select which of the supported 3Com devices in your network you wish to configure as follows (See Figure 74):

**Figure 74** Prioritize Network Traffic Wizard - Configuration Type



Prioritize Network Traffic Wizard

Configuration Type

Please specify the type of configuration you would like to apply by selecting the appropriate option below.

● Network-wide configuration

Applies the configuration to all supported 3Com devices in the network.

○ Device type configuration 3Com Switch 4200

Applies the configuration to all 3Com devices of the selected type in the network.

○ Custom configuration

Applies the configuration to selected device(s). This list will contain the current device selection.

Click Next to continue.

- **Network-wide Configuration** — applies the selected configuration to all of the supported 3Com devices in the current inventory file. 3Com recommends that you use this configuration type whenever you intend to make changes to your selection or when you are first configuring traffic prioritization on your network. If a new configuration is not applied across all of the devices then end-to-end traffic prioritization may not be possible.
- **Device Type Configuration** — applies the selected configuration to all of the devices of a specific type in the current inventory file. 3Com recommends that you only use this configuration type when you have added a large number of devices of a particular type to your network and you wish to configure them to participate in a previously configured end-to-end traffic prioritization.
- **Custom Configuration** — allows you to choose which of the supported 3Com devices in your network that the wizard should apply the selected configuration to. 3Com recommends that you only use this configuration type when you have added new devices to your network and you wish to configure them to participate in a previously configured end-to-end traffic prioritization.

### Servers Step

You can select servers for prioritization or blocking. In terms of the Prioritize Network Traffic Wizard, a server can be any device with an IP address regardless of whether or not the device is present in the 3Com Network Administrator inventory file. This enables you to perform actions such as blocking traffic to and from streaming media servers that are external to your company or to prioritize traffic to and from your partners websites.

- **Prioritized Servers** — when a server is prioritized, two things occur:
  - Traffic to or from the prioritized server will be treated as more important than non-prioritized traffic by the configured devices. Traffic will, therefore, flow through the network faster and with less chance of being dropped.
  - Prioritizing the server overrides application blocking, so a server selected for prioritization will still be able to use applications that are selected for blocking without the devices in the network dropping the application’s traffic.

3Com Network Administrator configures devices that are capable of classifying traffic based upon IP addresses to identify traffic going to or from a server selected for prioritization. This is achieved by creating classifier rules that match packets with either the destination or source IP address respectively set to the IP address of the server. Traffic that matches these classifier rules is mapped to the Business Critical service level. See "3Com Network Administrator Service Levels" on page 182 for definitions of the service levels used by 3Com Network Administrator.

When you are configuring devices that are not capable of classifying traffic based upon IP addresses, 3Com Network Administrator configures these devices to identify traffic with the Business Critical DiffServ codepoint. Traffic that matches this classifier rule is also mapped to the Business Critical service level.

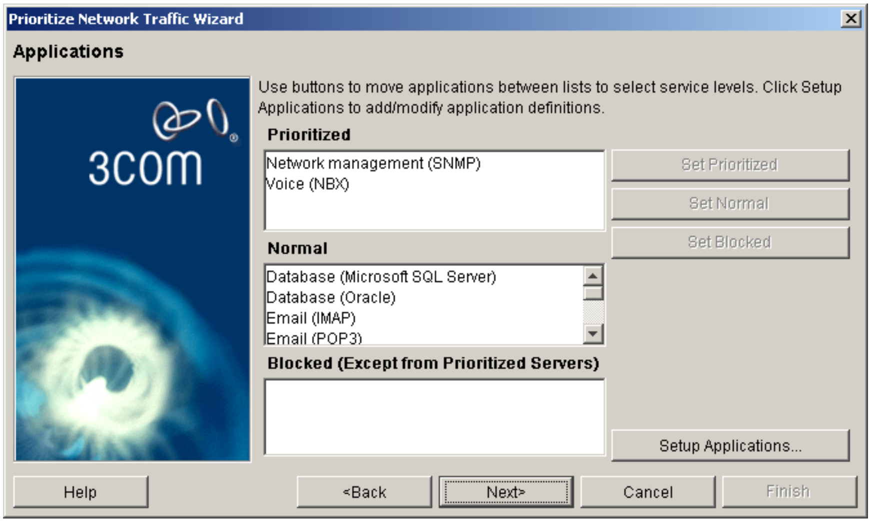
- **Blocked Servers** — selecting a server for blocking simply causes traffic to or from that server to be dropped by configured devices that are capable of both classifying traffic based upon IP addresses and of dropping traffic as a result of classification. 3Com Network Administrator configures these devices to identify traffic going to or from a server that has been selected for blocking. This is achieved by creating classifier rules that match packets with either the destination or source IP address respectively set to the IP address of the server. Traffic that matches these classifier rules is mapped to the Drop service level. See "3Com Network Administrator Service Levels" on page 182 for definitions of service levels used by 3Com Network Administrator.

  There are several servers that 3Com Network Administrator will not allow you to select for blocking. In addition, there are various problems that may arise due to selecting servers for blocking. For more information see "Potential Hazards When Blocking Traffic To and From Servers" on page 186.

### Applications Step

You can select applications for prioritization or blocking (See Figure 75). The Prioritize Network Traffic Wizard defines an application as a collection of classifier rules, each of which specifies one method of identifying traffic belonging to that application. These classifier rules specify the values that certain fields with a packet must have in order for that packet to be considered as belonging to the application.

**Figure 75** Prioritize Network Traffic Wizard - Applications



Prioritize Network Traffic Wizard

**Applications**

Use buttons to move applications between lists to select service levels. Click Setup Applications to add/modify application definitions.

**Prioritized**

Network management (SNMP)
Voice (NBX)

**Normal**

Database (Microsoft SQL Server)
Database (Oracle)
Email (IMAP)
Email (POP3)

**Blocked (Except from Prioritized Servers)**

*When a device is configured with the classifier rules for a particular application only one of the rules needs to match a packet in order for the packet to be identified as belonging to that application.*

- **Prioritized Applications** — when you select an application for prioritization, traffic identified as belonging to that application is treated as more important than non-prioritized traffic by the configured devices. This means that the traffic will flow through the network faster and with less chance of being dropped.

  3Com Network Administrator configures devices that are capable of performing complex application classification to identify traffic as belonging to an application by creating classifier rules. These classifier rules are equivalent to the classifier rules that make up the definition in the wizard. Traffic that matches these classifier rules is also mapped to the Business Critical service level. See "3Com Network Administrator Service Levels" on page 182 for definitions of the service levels used by 3Com Network Administrator.

  When you are configuring 3Com devices that are not capable of complex application classification, 3Com Network Administrator configures these devices to identify traffic with the Business Critical DiffServ codepoint. Traffic that matches this classifier rule is also mapped to the Business Critical service level.

- **Blocked Applications** — selecting an application for blocking causes traffic identified as belonging to that application to be dropped. Not all devices are capable of dropping application traffic. A device must be capable of both complex application classification and of dropping traffic as a result of classification in order to drop application traffic. 3Com Network Administrator configures such devices to identify traffic as belonging to an application by creating classifier rules. These classifier rules are equivalent to the classifier rules that make up the definition in the wizard. Traffic that matches these classifier rules is mapped to the Drop service level. See "3Com Network Administrator Service Levels" on page 182 for definitions of the service levels used by 3Com Network Administrator.

*3Com* Network Administrator *imposes restrictions on the blocking of SNMP traffic. In addition, there are various problems that may arise due to selecting applications for blocking. For more information see* "Potential Hazards of Blocking Application Traffic" *on* page 188*.*

*If you prioritize traffic to and from a server then that server will also be able to use any applications that are blocked.*

### Application Field Values

Application traffic is identified by examining certain fields in the packets to see if they contain specific values. If you wish to add an application that is not present in the list you will need to know the appropriate field values required for that application.

*More information on how to determine the appropriate field values is available in* "Determining Field Values for Applications" *on* page 182*.*

### Finish Step and Progress

Changes to your network traffic prioritization configuration are not applied to your network until you select *Finish* on the Configuration *Summary* dialog. After selecting *Finish*, the Prioritize Network Traffic Wizard configures each of the supported 3Com devices in the inventory file to prioritize network traffic according to your selected configuration. During the configuration of the devices, the *Configuring Prioritization* dialog is shown to indicate the progress.

You can cancel the configuration at any time. If you do cancel, the wizard will complete the configuration of the devices it was in the process of configuring before aborting. However, the configuration may then result in an inconsistent configuration across your network and so traffic may not receive end-to-end traffic prioritization. As a result, it is recommended that you do not cancel the configuration once it has started.

## Prioritization Reports

The following reports are produced through the traffic prioritization feature:

### Agent Upgrades Required for Prioritization Report

The Prioritize Network Traffic Wizard analyzes the details of your device inventory to determine what devices the wizard can configure. If devices cannot be supported for either agent version or licensing reasons, it will inform you of this problem and subsequently generate an Agent Upgrades Required for Prioritization report.

For each device that the wizard cannot support due to its agent version, the report lists the following details:

- Device name
- Device type
- IP address
- The agent version that the device is currently running
- The minimum agent version that the device must be running for the wizard to configure traffic prioritization.

For each device that the wizard cannot support due to licensing reasons, the report lists:

- Device name
- Device type
- IP address

### Network Prioritization Report

The Prioritize Network Traffic Wizard automatically generates a Network Prioritization report after it has completed the configuration of your network for traffic prioritization. The Network Prioritization report details the following:

- The servers whose traffic has been prioritized.
- The applications whose traffic has been prioritized.
- The servers whose traffic the network has been configured to block.
- The list of applications whose traffic the network has been configured to block.
- The devices in the network that were successfully configured.
- The devices in the network that the wizard failed to configure. 3Com Network Administrator reports a reason for each failure.
- Detailed information about the configuration applied to the devices, including any restrictions as to what the devices will do in terms of prioritization and blocking.

### Prioritization Configuration Report

If you wish to view the details of the configurations in terms of classifiers, queuing, dropping and marking, run the Prioritization Configuration report. This report can be run by selecting *Tools > Reports*.

For each device that the report is run against, the Prioritization Configuration report lists:

- The classifiers that are in use on each port
- The service levels that the classifiers map to
- The details of each classifier that is currently in use on the device
- The details of each service level that is currently in use on the device

The report can help you determine whether you have applied a consistent end-to-end traffic prioritization configuration in your network. This is particularly useful if you have decided to manually configure your devices.

*Whenever you run the Prioritization Configuration report, 3Com Network Administrator retrieves the configuration information directly from the supported 3Com devices in your network. As this report must poll each of the devices for data it may take several minutes to run.*

## Examples

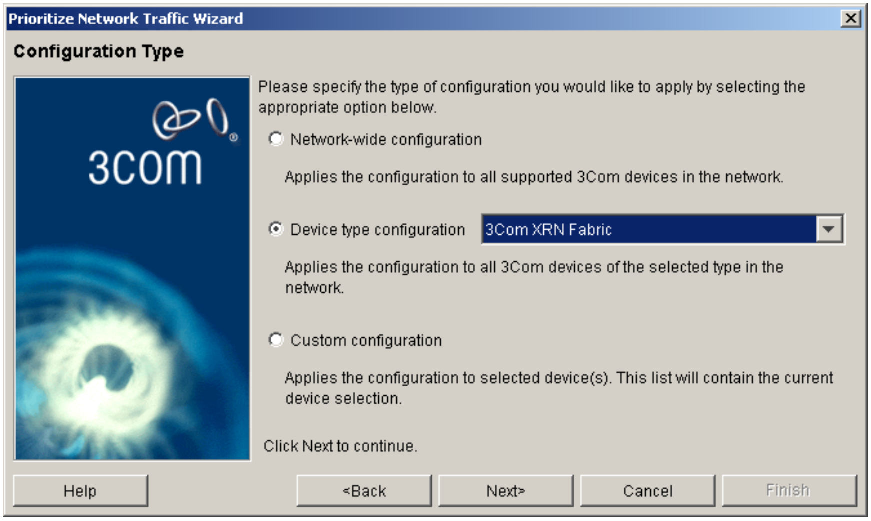
The following section details useful examples of traffic prioritization configuration.

### Applying an Existing Configuration to New Devices

You have just upgraded the core of your network to an XRN core and wish to configure the XRN devices to participate in the end-to-end prioritization configuration that you have previously applied to your network. To do this:

1. Ensure that the new devices are present in the inventory file by importing an updated list of devices from HP OpenView, if necessary.
2. In the *Introduction* step, select *Next*. The wizard will analyze the devices in the inventory file and display the *Configuration Type* step as shown in Figure 76.

**Figure 76** Configuration Type - Applying an Existing Configuration to New Devices Example



Prioritize Network Traffic Wizard

Configuration Type

Please specify the type of configuration you would like to apply by selecting the appropriate option below.

○ Network-wide configuration

Applies the configuration to all supported 3Com devices in the network.

● Device type configuration: 3Com XRN Fabric

Applies the configuration to all 3Com devices of the selected type in the network.

○ Custom configuration

Applies the configuration to selected device(s). This list will contain the current device selection.

Click Next to continue.

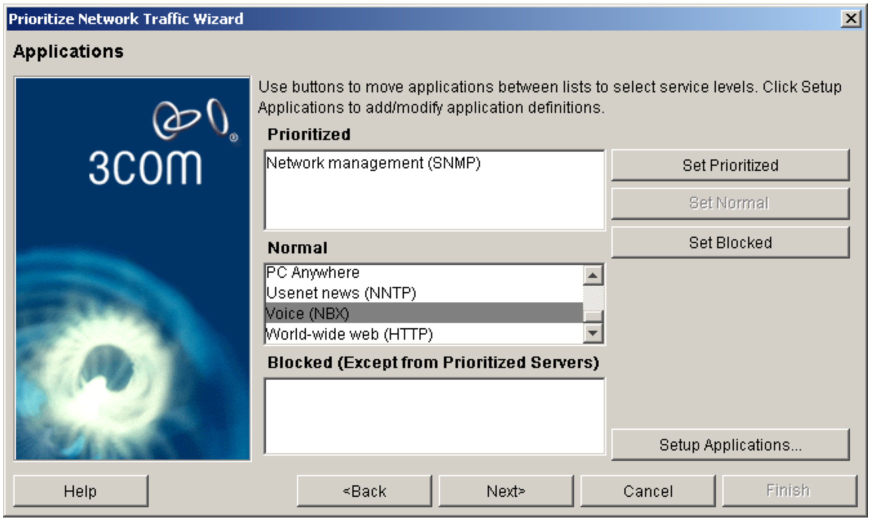
3. Click the *Device type configuration* radio button and select *3Com XRN Fabric* from the drop-down list.
4. Click *Next* to show the *Servers* step in the wizard and continue selecting *Next* until the *Configuration Summary* step is shown.
5. Click *Finish* to apply the previously applied configuration to your XRN core.

## Prioritizing NBX Voice Traffic

You have recently installed an NBX phone system in your network and wish to ensure that the phone calls made using the system are of high quality, even when the network is congested. To do this:

1 In the *Introduction* step, select *Next*. The wizard will analyze your network and display the *Configuration Type* step as shown in Figure 77.

**Figure 77** Configuration Type - Prioritizing NBX Voice Traffic Example



Prioritize Network Traffic Wizard

Applications

Use buttons to move applications between lists to select service levels. Click Setup Applications to add/modify application definitions.

Prioritized

Network management (SNMP)

Normal

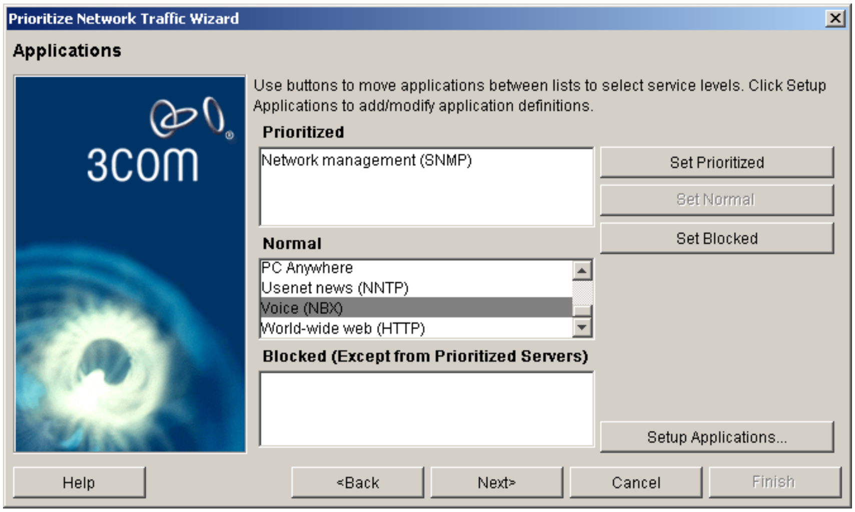
PC Anywhere
Usenet news (NNTP)
Voice (NBX)
World-wide web (HTTP)

Blocked (Except from Prioritized Servers)

2 Click the *Network-wide configuration* radio button and click *Next* to show the *Servers* step.

3 Click *Next* to show the *Applications* step as shown in Figure 78.

**Figure 78** Applications - Prioritizing NBX Voice Traffic Example



Prioritize Network Traffic Wizard

**Applications**

Use buttons to move applications between lists to select service levels. Click Setup Applications to add/modify application definitions.

**Prioritized**

Network management (SNMP)

**Normal**

PC Anywhere
Usenet news (NNTP)
Voice (NBX)
World-wide web (HTTP)

**Blocked (Except from Prioritized Servers)**

4 Select the *Voice (NBX)* application from the *Normal* list and then click *Set Prioritized*.

5 Click *Next* to show the next step of the wizard. If the *Resource Warning* dialog is displayed then you may wish to resolve the resource warnings before proceeding. Refer to "Resource Warnings" on page 184 for more information.

6 When you reach the *Configuration Summary* step, select *Finish* to apply the updated configuration to the supported 3Com devices in the inventory file.

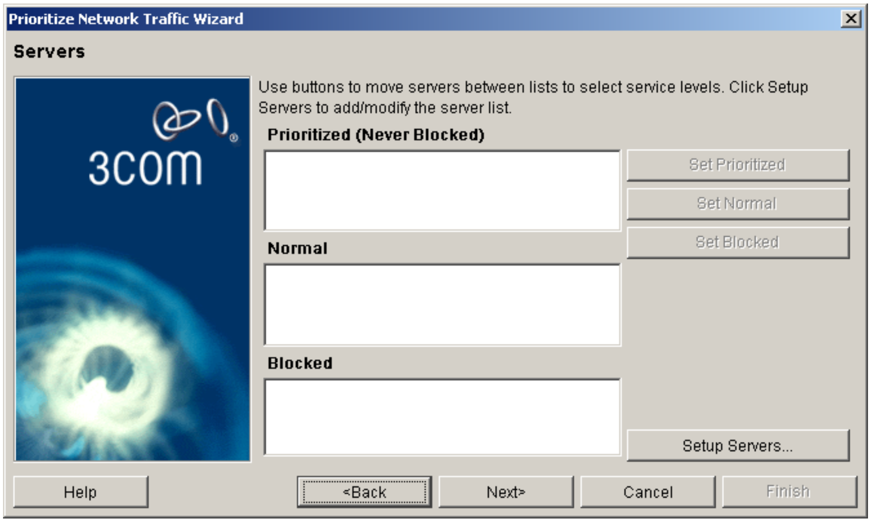
## Prioritizing Traffic To and From a SAP Server

You have noticed that during periods of network congestion, several of your users have had difficulties accessing your SAP server. As this is having an impact on your business, you wish to prioritize traffic to and from the server to prevent these difficulties from arising.

1 In the *Introduction* step, select *Next*. The wizard will analyze your network and display the *Configuration Type* step as shown in Figure 77.

2 Select the *Network-wide configuration* radio button and select *Next* to show the *Servers* step as shown in Figure 79.

**Figure 79** Servers - Prioritizing Traffic To and From a SAP Server Example



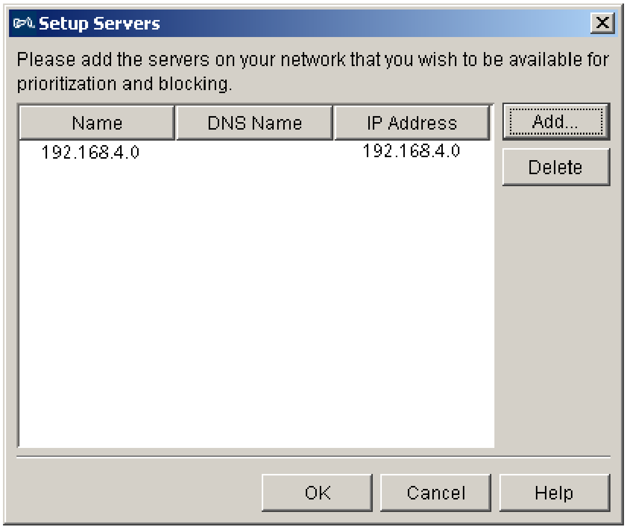
Prioritize Network Traffic Wizard

**Servers**

Use buttons to move servers between lists to select service levels. Click Setup Servers to add/modify the server list.

3 To add the SAP server to the list of servers, select *Setup Servers* from the *Servers* step to display the *Setup Servers* dialog as shown in Figure 80.

**Figure 80** Setup Servers - Prioritizing Traffic To and From a SAP Server Example



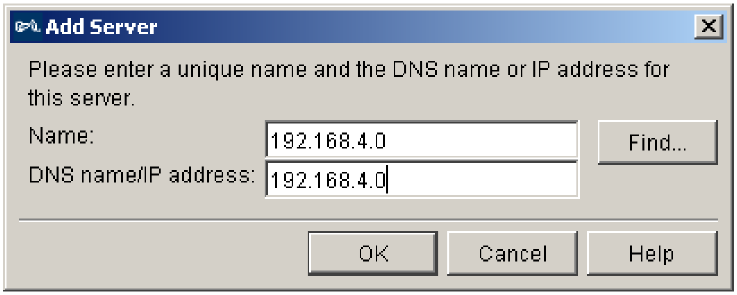
Setup Servers

Please add the servers on your network that you wish to be available for prioritization and blocking.

| Name | DNS Name | IP Address |
|---|---|---|
| 192.168.4.0 | | 192.168.4.0 |

4 In the *Setup Servers* dialog, select *Add* to display the *Add Server* dialog (as shown in Figure 81) enabling you to add the SAP server.

**Figure 81** Add Server - Prioritizing Traffic To and From a SAP Server Example



Please enter a unique name and the DNS name or IP address for this server.

Name: 192.168.4.0

DNS name/IP address: 192.168.4.0

5 Type the name of the SAP server (or the function that it performs) into the *Name:* field and type either the DNS name or the IP address of the server into the *DNS name/IP address:* field. Select *OK* to add the server and return to the *Setup Servers* step.

If you have entered a DNS name then 3Com Network Administrator will resolve the DNS name to an IP address for you.

6 Select *OK* in the *Setup Servers* step to return to the *Servers* step where the SAP server is now listed in the *Normal* list.

7 Select the SAP server from the *Normal* list and select *Set Prioritized* then select *Next* to display the *Applications* step.

8 Select *Next* to show the next step of the wizard. If the *Resource Warning* dialog is displayed you may wish to resolve the resource warnings before proceeding. Refer to "Resource Warnings" on page 184 for more information.

9 When you reach the *Configuration Summary* step, select *Finish* to apply the updated configuration to the supported 3Com devices in the inventory file.

## Blocking Access to a Streaming Audio Server

You have noticed that a significant amount of traffic is going to and from a server that provides streams for internet radio stations. This traffic is having an adverse effect upon other traffic and you wish to temporarily prevent access to the streaming audio server.

1 In the *Introduction* step, click *Next*. The wizard will analyze your network and display the *Configuration Type* step as shown in Figure 77

2 Select the *Network-wide configuration* radio button and click *Next* to show the *Servers* step shown in Figure 79.

3 To add the streaming audio server to the list of servers, click *Setup Servers* from the *Servers* step to display the *Setup Servers* dialog in Figure 80.

4 In the *Setup Servers* dialog, click *Add* to display the *Add Server* dialog in Figure 81, enabling you to add the streaming audio server.

5 Type the name of the streaming audio video server (or the function that it performs) into the *Name:* field and type either the DNS name or the IP address of the server into the *DNS name/IP address* field. Select *OK* to add the server and return to the *Setup Servers* step.

   If you have entered a DNS name then 3Com Network Administrator will resolve the DNS name to an IP address for you.

6 Click *OK* in the *Setup Servers* step to return to the *Servers* step where the streaming audio server is now listed in the *Normal* list.

7 Select the streaming audio server from the *Normal* list and select *Set Blocked* and dismiss the warning dialog that is displayed.

8 Click *Next* to display the *Applications* step.

9 Click *Next* to display the next step of the wizard. If the *Resource Warning* dialog is displayed then you may wish to resolve the resource warning before proceeding. Refer to "Resource Warnings" on page 184 for more information.

10 When you reach the *Configuration Summary* step, click *Finish* to apply the updated configuration to the supported 3Com devices in the inventory file.

## Prioritizing a Video Conferencing Application

The CEO is holding a video conference with direct reports over the corporate intranet. Previous conferences like this have been affected by network congestion causing intermittent loss of video and audio. You decide to prioritize the traffic belonging to the video conferencing application to prevent similar disruption to this conference.

You have determined that your video conferencing software uses UDP port 2001 for audio, UPD port 2002 for video and 2003 for signaling.

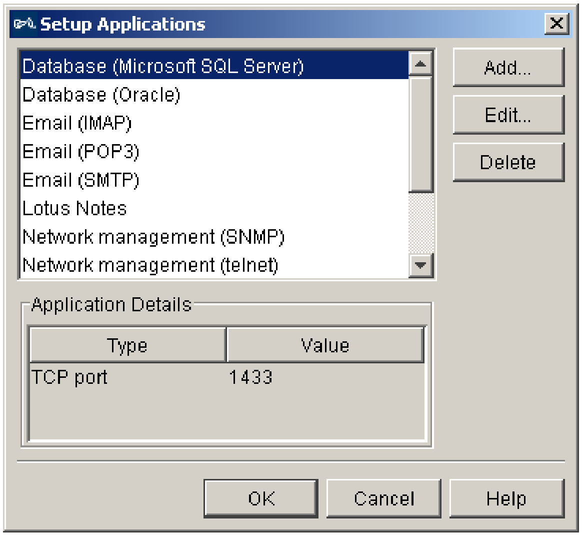
1 In the *Introduction* step, click *Next*. The wizard will analyze the devices in the current inventory file and display the *Configuration Type* step as shown in Figure 77.

2 Select the *Network-wide configuration* radio button and select *Next* to display the *Servers* step.

3 Click *Next* to display the *Applications* step as shown in Figure 78.

**4** To add the video conferencing application to the list of applications, select *Setup Applications* from the *Applications* step to display the *Setup Applications* dialog in Figure 82.

**Figure 82** Setup Applications - Prioritizing a Video Conferencing Application Example



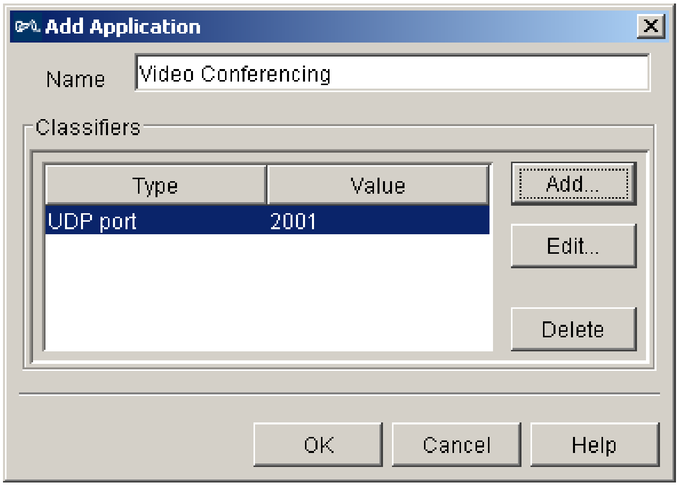
Database (Microsoft SQL Server)
Database (Oracle)
Email (IMAP)
Email (POP3)
Email (SMTP)
Lotus Notes
Network management (SNMP)
Network management (telnet)

Application Details

| Type | Value |
|---|---|
| TCP port | 1433 |

**5** Click *Add* to display the *Add Applications* step as shown in Figure 83.

**Figure 83** Add Applications - Prioritizing a Video Conferencing Application Example



Name: Video Conferencing

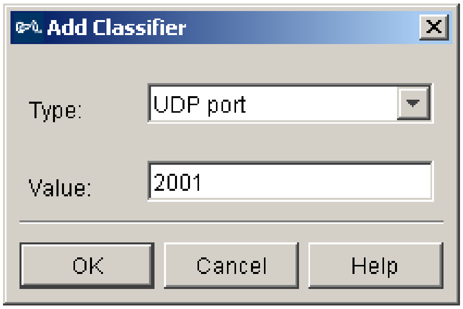
Classifiers

| Type | Value |
|---|---|
| UDP port | 2001 |

6 To specify the application definition, type the name of the application in the *Name* field.

7 To add each of the classifiers to the application, click *Add* to display the *Add Classifier* dialog as shown in Figure 84.

**Figure 84** Add Classifier - Prioritizing a Video Conferencing Application Example



Type: UDP port

Value: 2001

8 Select the appropriate type and enter the appropriate value (in this case, UDP and 2001 respectively). Click *OK* to return to the *Setup Application* step.

9 Repeat steps 7 and 8 to add in the remaining classifiers (in this case, UDP port 2002 and UDP port 2003).

10 Click *OK* again to return to the *Applications* dialog where the video conferencing application is now listed in the *Normal* list.

11 Select the video conferencing application from the *Normal* list. Select *Set Prioritized*.

12 Click *Next* to display the next step of the wizard. If the *Resource Warning* dialog is displayed then you may wish to resolve the resource warning before proceeding. Refer to "Resource Warnings" on page 184 for more information.

13 When you reach the *Configuration Summary* step, click *Finish* to apply the updated configuration to the supported 3Com devices in the inventory file.

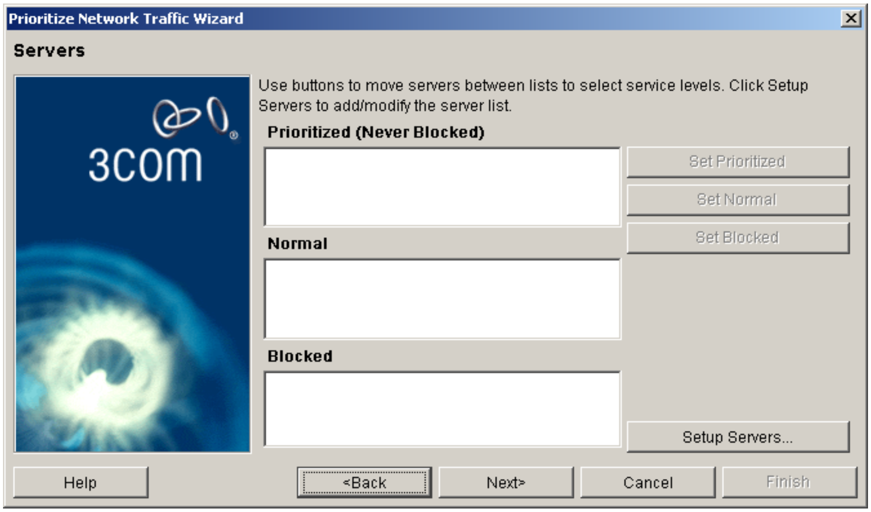
## Restricting Access to SNMP

For security purposes you wish to restrict the use of SNMP in your network to the PCs used by the network managers

**1** In the *Introduction* step, click *Next*. The wizard will analyze the devices in your inventory file and display the *Configuration Type* step as shown in Figure 77.

**2** Select the *Network-wide configuration* radio button and click *Next* to display the *Servers* step as shown in Figure 85.

**Figure 85** Servers - Restricting Access to SNMP Example



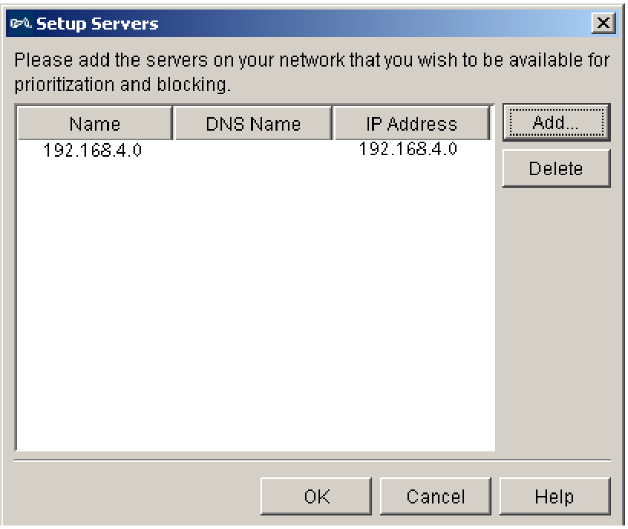
Prioritize Network Traffic Wizard

**Servers**

Use buttons to move servers between lists to select service levels. Click Setup Servers to add/modify the server list.

**3** To add the first network managers' PC to the list of servers, select *Setup Servers* from the *Servers* step to display the *Setup Servers* dialog in Figure 86.

**Figure 86** Setup Servers - Restricting Access to SNMP Example



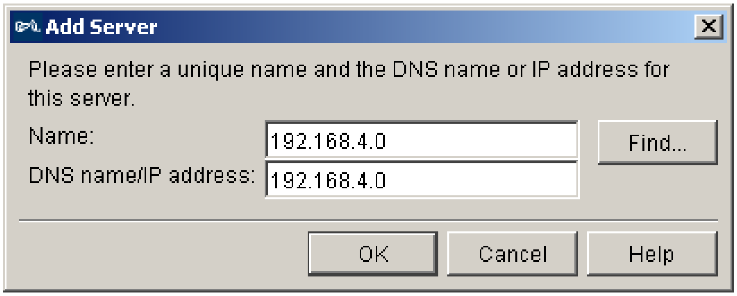
Setup Servers

Please add the servers on your network that you wish to be available for prioritization and blocking.

| Name | DNS Name | IP Address |
|---|---|---|
| 192.168.4.0 | | 192.168.4.0 |

4 In the *Setup Servers* dialog, click *Add* to display the *Add Server* dialog in Figure 87, enabling you to add the first network managers' PC.

**Figure 87** Add Server - Restricting Access to SNMP Example



Add Server

Please enter a unique name and the DNS name or IP address for this server.

Name: 192.168.4.0

DNS name/IP address: 192.168.4.0

5 Type the name of the PC (or the function that it performs, or the name of the network manager) into the *Name:* field and type either the DNS name or the IP address of the PC into the *DNS name/IP address:* field. Click *OK* to add the PC and return to the *Setup Servers* dialog.

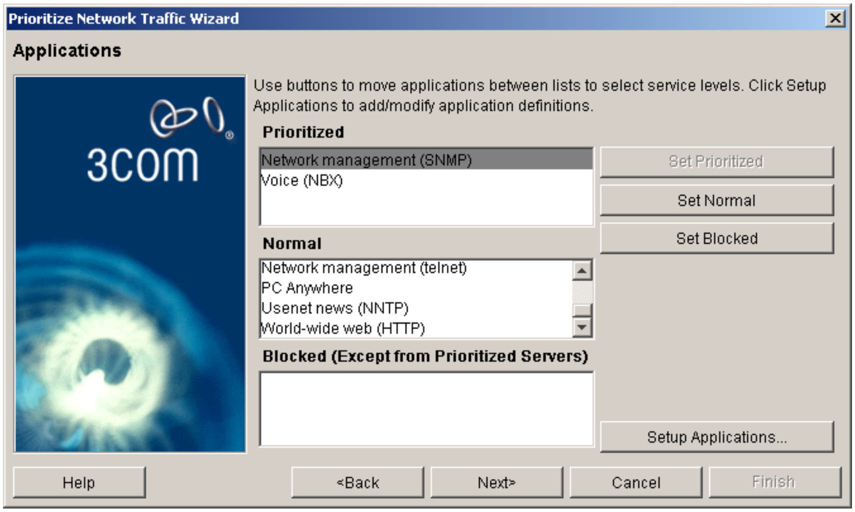
If you have entered a DNS name then 3Com Network Administrator will resolve the DNS name to an IP address for you.

6 Repeat steps 4 and 5 to add in the other network managers' PCs.

7 Click *OK* in the *Setup Servers* step to return to the *Servers* step where the network managers' PCs are now listed in the *Normal* list.

8 Select all of the network managers' PCs from the *Normal* list and select *Set Prioritized*, then select *Next* to display the *Applications* step as shown in Figure 88.

**Figure 88** Applications - Restricting Access to SNMP Example



Prioritize Network Traffic Wizard

Applications

Use buttons to move applications between lists to select service levels. Click Setup Applications to add/modify application definitions.

Prioritized

- Network management (SNMP)
- Voice (NBX)

Normal

- Network management (telnet)
- PC Anywhere
- Usenet news (NNTP)
- World-wide web (HTTP)

Blocked (Except from Prioritized Servers)

9 Select the application *Network Management (SNMP)* from the *Normal* or *Prioritized* list. Select *Set Blocked* and dismiss the warning dialog that is displayed.

10 Click *Next* to display the next step of the wizard. If the *Resource Warning* dialog is displayed then you may wish to resolve the resource warning before proceeding. Refer to "Resource Warnings" on page 184 for more information.

11 When you reach the *Configuration Summary* step, click *Finish* to apply the updated configuration to the supported 3Com devices in the inventory file.

## Useful Information and References

The following section provides useful information and references when using the Prioritizing Network Traffic feature of 3Com Network Administrator.

### User Priority Field

The user priority field (and the tagged header that it is present in) allows information about the priority level of a packet to be carried with the packet as it traverses the network. The field is defined with the IEEE (Institute of Electrical and Electronics Engineers) 802.1D standard, which is available from the IEEE website:

`http://www.ieee.org/`

This standard defines the use of the eight values that the field may take. These definitions are shown in Table 17.

**Table 17** User Priority

| User Priority | Use |
|---|---|
| 1 | Background |
| 2 | Spare |
| 0 (Default) | Best Effort |
| 3 | Excellent Effort |
| 4 | Controlled Load |
| 5 | "Video," < 100 ms latency and jitter |
| 6 | "Voice," < 10 ms latency and jitter |
| 7 | Network Control |

As the table shows, the default value is 0. This allows some traffic to be marked as less important than normal traffic.

The tagged header that the user priority field relies upon can be used in any packet in place of the normal 802.1D header. However, the tagged header is only normally used for packets if VLANs are being used within the network. This means that if VLANs are not being used then the information about the importance of traffic cannot be conveyed from a complex classification device to a simple classification device using this marking mechanism.

## DiffServ Codepoint Field

The DiffServ Codepoint field, defined in the IETF (Internet Engineering Task Force) RFC 2474, allows information about the quality of service requirements of a packet to be carried with the packet as it traverses the network.

There are no restrictions on what any of the codepoint values mean as it is the choice of the network manager or the network management tool to decide the local meanings, although there are recommended uses for some of the values. The codepoint meanings can extend beyond simple traffic priority to more precise specifications such as latency and jitter requirements.

Information about the field, its use and the recommended values are available in the IETF RFCs listed in Table 18.

**Table 18** RFC Definitions

| RFC Number | Title |
|---|---|
| RFC 2474 | Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers |
| RFC 2475 | An Architecture for Differentiated Services |
| RFC 2597 | Assured Forwarding PHB Group |
| RFC 3246 | An Expedited Forwarding PHB |
| RFC 3247 | Supplemental Information for the New Definition of the EF PHB |
| RFC 3260 | New Terminology and Clarification for DiffServ |

All of these RFCs are freely available from the IETF website:

**`http://www.ietf.org/`**

The RFCs listed in Table 18 do not include all of the RFCs relevant to DiffServ. Additional RFCs can be located on the Differentiated Services Working Group’s page on the IETF website.

As the DiffServ codepoint field is only present in IP packets, this restricts the use of this marking mechanism to IP packets only. This means that the information about the importance of non-IP traffic cannot be conveyed from a complex classification device to a simple classification device using this marking mechanism.

## Determining Field Values for Applications

In order to create a new application definition, it is necessary to know the field values that can be used to identify that application. Many vendors now provide the information about the field values that their applications use either in the application manual or on the vendor's website to aid firewall configuration. This information may also be used for creating the application definition within the Prioritize Network Traffic Wizard.

If you cannot find the information from either the application manual or the vendor's website then there are various other websites that may provide the information that you require. In particular, the IEEE are responsible for allocating Ethernet type values. A list of the assigned Ethernet type values can be found on the IEEE website:

`http://www.ieee.org/`

Similarly, as IANA (Internet Assigned Number Authority) are responsible for allocating TCP and UDP port numbers, a list of known TCP and UDP port numbers can be found on the IANA website:

`http://www.iana.org/`

The IANA website also contains a list of the known IP protocol numbers.

## 3Com Network Administrator Service Levels

3Com Network Administrator uses the service levels on the devices it configures as shown in Table 19.

**Table 19** Service Levels Used by 3Com Network Administrator

| Service Level | Queue | | Marking Value | |
|---|---|---|---|---|
| | **2 Queue Device** | **4 Queue Device** | **802.1p** | **DSCP** |
| Voice | 1 (High) | 3 (High) | 6 | 46 |
| Business Critical | 1 (High) | 1 | 3 | 16 |
| Drop | ------------------ Traffic is dropped ------------------ | | | |

The classifiers created by 3Com Network Administrator are mapped to these service levels as follows:

- Classifiers created for NBX traffic are mapped to the Voice service level.
- Classifiers created for applications or servers that have been selected for prioritization are mapped to the Business Critical service level.

- Classifiers created for applications or servers that have been selected for blocking are mapped to the Drop service level.
- All other traffic is left unclassified and is treated with the Default service level. This service level does not perform any remarking and sends all packets to queue 0 (Low).

## Configuration Levels for Supported 3Com Devices

The Prioritize Network Traffic Wizard configures devices based upon their capabilities. These capabilities are dependent upon the device type and the agent software version.

Table 20 summarizes how the wizard will configure the supported devices:

**Table 20** Configuration Levels for Supported 3Com Devices

| Device Type | Agent Version | Classify Servers | Classify Applications | Drop Traffic | Number of Queues | Mark 802.1p | Mark DSCP |
|---|---|---|---|---|---|---|---|
| SuperStack 3 Switch 4200 Family | Any | ✕ | ✕ | ✕ | 2 | ✕ | ✕ |
| SuperStack 3 Switch 4400 Family | Any | ✓ | ✓ | ✓ | 4 | ✓ | ✓ |
| SuperStack 3 Switch 4900<br>SuperStack 3 Switch 4900SX | 2.0 or later | ✕ | ✕ | ✕ | 4 | ✓ | ✕ |
| Superstack 3 Switch 4924<br>Superstack 3 Switch 4950 | 2.0 | ✕ | ✕ | ✕ | 4 | ✓ | ✕ |
| Superstack 3 Switch 4924<br>Superstack 3 Switch 4950 | 2.5 or later | ✓ | ✕ | ✓ | 4 | ✓ | ✓ |
| Switch 4050<br>Switch 4060 | Any | ✓ | ✕ | ✓ | 4 | ✓ | ✓ |

*If a device is listed as not supporting 'Classify Servers' or 'Classify Applications' and you select a server or an application for prioritization, the wizard will create a classifier for the Business Critical service level's DiffServ codepoint value and map it to the Business Critical service level instead.*

*If a device is listed as supporting 'Drop Traffic' it will only be configured to drop traffic to and from servers selected for blocking if it is listed as supporting 'Classify Servers'. Similarly, a device will only be configured to drop traffic for applications selected for blocking it if is listed as supporting 'Classify Applications'.*

## Key Considerations

The following section provides assistance when configuring traffic prioritization on your network:

### Resource Warnings

Resource warnings occur for the following reasons:

- Each device type has a certain number of resources available for classification which are managed in different ways by different device types. If a particularly complex configuration is selected then it may not be possible to configure all of the supported devices to match the configuration exactly as the configuration may require more resources than are available on some or all of the selected devices.
- On some devices the classification functionality may differ depending on the agent version running on that device. Similarly, it is not possible to configure a device to exactly match a configuration that requires a certain level of classification functionality if the appropriate agent is not installed on the device.

If either of these situations occur a *Resource Warning* dialog is displayed prior to the *Configuration Summary* step. The dialog will list each distinct problem that has been detected as shown in Table 21.

**Table 21** Resource Warnings

| Resource Warning Content | Explanation (if appropriate) |
|---|---|
| The type of devices that are affected by this problem | |
| A description of the problem | If the problem is resource related then a percentage indication will be given of the attempted resource usage. |
| A list of all devices that are affected by this problem | |
| Details of the problem | If the problem is resource related then the percentage resource requirements of each server and application selected for prioritization or blocking will be shown. |
| The reduced configuration that will be applied if the problem is not resolved | In many cases the reduced configuration will be equivalent to treating the affected devices as if they were not capable of complex configuration. If you were to proceed with the configuration without resolving the resource warnings, these devices would only be able to perform traffic prioritization if the traffic had first passed through a device that had been configured to perform complex classification and marking. |
| A suggested resolution to the problem | If the problem is resource related then it can be resolved by reducing the complexity of the configuration. If the problem is due to the agent version then it can be resolved by updating the agent to at least the minimum agent version suggested in the warning. |

*If any of the resource warnings are due to the agent versions running on your devices then you can use* Tools > Agent Update *to find and update all devices whose agent software version is out of date.*

*If you proceed with the configuration without resolving the resource warnings then the reduced configuration that is applied to your network may not be capable of performing any complex classification. If this is the case then you will effectively have no traffic prioritization in your network.*

## Why Errors Can Occur When Adding a Server

When you are adding a server it is necessary to enter a unique non-blank name and either a valid DNS name or a valid IP address. If you choose to enter an IP address it must not be a broadcast IP address. If any of these conditions are not met then the wizard will not allow the server to be added and an appropriate warning message will be displayed.

3Com Network Administrator will resolve DNS names by using the DNS servers that the PC it is running on is configured to use and that 3Com Network Administrator was able to contact when it was started. This means that you will be unable to add servers by DNS name if any of the following occur:

- 3Com Network Administrator was unable to contact any of the configured DNS servers when it was started.
- 3Com Network Administrator was only able to contact some of the configured DNS servers when it was started and none of the DNS servers contacted are able to resolve the DNS name.
- It is not possible to contact any of the configured DNS servers while you were adding servers.
- It is only possible to contact some of the configured DNS servers while you were adding servers and none of the DNS servers that can be contacted are able to resolve the DNS name.

If it was not possible to contact a DNS server when 3Com Network Administrator was started but you are now able to do so, you will need to restart 3Com Network Administrator before it will use the DNS server.

## Potential Hazards When Blocking Traffic To and From Servers

Blocking traffic to and from servers is a powerful feature that prevents access to particular resources. However, if you select the wrong servers to be blocked then this can cause severe problems on your network.

Whenever you attempt to block traffic to and from a server it is important that you check that:

- The IP address of the server you wish to block does not belong to a server that is critical to your network infrastructure, such as a DHCP or RADIUS server. Blocking IP addresses such as these may prevent your network infrastructure from functioning correctly.

- The IP address of the server that you wish to block does not belong to a server that is critical to your business, such as a database or email server. Blocking IP addresses such as these may have a major impact on your business.
- The IP address of the server that you wish to block is not an IP address that is served by a DHCP server. A device that has an IP address that is served by a DHCP server can potentially change and this could lead to intermittent problems for users of your network. If one or more of the network infrastructure devices on your network obtained their addresses via DHCP it could prevent your network from functioning correctly.

If you have previously configured the network to block traffic to and from a server it is important that prior to assigning an IP address to a new device (or any existing device whose IP address you wish to change) you check that the IP address that you are about to assign is not an IP address of a server you have blocked. One way to check this is to run the Prioritization Configuration report by selecting *Tools* > *Reports* and examining the contents of the report for blocked servers.

If you accidently block an IP address then you can rectify this problem by re-running the Prioritize Network Traffic Wizard and removing the server from the list of servers to be blocked.

### Servers That Cannot be Selected for Blocking

3Com Network Administrator prevents you selecting the following servers for blocking:

- The PC that is running 3Com Network Administrator. If you attempted to block this server 3Com Network Administrator would no longer be able to contact your network. This would prevent it from configuring the devices on your network.
- Any device in the device inventory that forms part of the network infrastructure, such as a switch, hub or router.

*3Com Network Administrator will not prevent you from blocking traffic to and from a device that is not listed in the device inventory. If any of your network infrastructure devices are not listed in the device inventory you will need to check that you have not accidently selected one of these devices for blocking before configuring traffic prioritization on your network.*

## Potential Hazards of Blocking Application Traffic

Blocking traffic belonging to applications is a powerful feature for preventing the use of undesired applications on your network. However, if the wrong application definitions are used for blocking an application this can cause severe problems on your network.

There are two reasons why blocking a particular application definition may cause problems on your network:

- The application definition may not be narrow enough to prevent accidental classification of other application traffic. For example, if an application runs over TCP/IP then specifying a classifier rule of 'IP protocol 6' (the protocol number of TCP) in the application definition would not be narrow enough for blocking as this would also block all other TCP/IP traffic.

  When blocking an application it is important that the definition is as specific as it can be about how to identify traffic belonging to that application. In the example above, it would be better in this case to specify the classifier rule of 'TCP port 123', assuming that the application uses TCP port 123, as this would only match and so only block TCP/IP traffic using port 123 rather than all TCP/IP traffic.
- The application definition, while still being narrow, may include rules that will incorrectly classify other applications as belonging to the application you wish to block. For example, if the definition for an application 'A' that you wish to block specifies the classifiers 'TCP port 123' and 'TCP port 456' and there is another application 'B' running in your network that uses TCP port 456, then blocking application A would also block application B.

  For many applications, it is enough to block only some of the traffic that the application generates in order to prevent if from running successfully on the network. Removing the classifiers that overlap with other applications may mean that you are still able to block the application. In the example above, it may be enough to only block TCP port 123 in order to prevent application A from running on your network and this would still allow application B to function correctly.

***CAUTION:*** *Many TCP and UDP based applications use dynamic port assignment to determine the TCP or UDP port that will be used as the source port. If your application definition contains a classifier for a TCP or UDP port that falls within a range that one or more of your devices may dynamically allocate to an application it could cause intermittent problems on your network. Whenever an application is dynamically allocated a port that is blocked it will be unable to function correctly.*

***CAUTION:*** *Some applications allow the user to select the protocols and ports that are used. Whilst blocking the default protocol and port settings for this type of application will prevent an 'out-of-the-box' instance from functioning correctly on your network, it cannot be guaranteed that this will block all instances of the application. Other instances may have been configured to use other protocols and ports.*

## Potential Hazards of Blocking SNMP, HTTP and Telnet

The protocols SNMP, HTTP and Telnet are all used for network management purposes. 3Com Network Administrator uses SNMP to configure its devices and, in some cases, can use HTTP and Telnet for device discovery and configuration. HTTP and Telnet protocols are also used for manual configuration of devices. Blocking an application whose definition includes the ports used by these protocols would prevent 3Com Network Administrator from functioning correctly and prevent you from manually accessing these devices.

*3Com Network Administrator will prevent you from blocking any application whose definition includes classifiers for the SNMP protocol unless you have first selected the PC that it is running on for prioritization. This is so that 3Com Network Administrator can continue to manage your network whilst SNMP is blocked.*

*By prioritizing the traffic of your network management PCs and by blocking SNMP you can prevent any unauthorized SNMP access on your network.*

# 9 REPORTING

## Overview

This chapter describes the Reporting feature of 3Com Network Administrator.

You can use the Reporting feature to obtain on-demand reports describing the 3Com devices on your network, listing attributes such as IP addresses, MAC addresses and agent software versions. You can also obtain specific information you may require by creating custom reports.

Reports are generated in HTML format to allow viewing using a web browser. You can export reports to CSV so that they can be imported into other tools such as Microsoft Excel or used in command line scripts.

You may view any report you have generated in the past by using the Reporting history.

The following topics are covered in this chapter:

- Key Concepts
- Components
- Examples
- Useful Information and References
- Key Considerations

## Key Concepts

This following section explains the key concepts of the Reporting feature.

### Selection-sensitive

Many reports may be launched against the current selection in the inventory, allowing you to generate reports listing only the devices you are interested in. Alternatively, you can choose to generate a report based on the whole inventory.

### Feature Reports

Various features within 3Com Network Administrator use reports to convey information. These are covered in the chapter detailing the feature as shown in Table 22:

**Table 22** Feature Reports

| Feature | Reports | Covered in: |
|---|---|---|
| Agent Update | ■ Agent Audit<br>■ Agent Update Summary | "Agent Update" on page 135 |
| Backup | ■ Backup Audit<br>■ Backup Summary | "Backup, Restore and Setup" on page 107 |
| Setup | Setup Summary | "Backup, Restore and Setup" on page 107 |
| Restore | Restore Summary | "Backup, Restore and Setup" on page 107 |
| Traffic Prioritization | ■ Prioritization Configuration<br>■ Network Prioritization<br>■ Agent Upgrades Required for Prioritization | "Prioritizing Network Traffic" on page 153 |
| Live Update | Live Update Activity | "Live Update" on page 221 |
| Agent Update, Backup, Restore and Setup | Device History | "Agent Update" on page 135<br>"Backup, Restore and Setup" on page 87 |

Other reports are covered in "Components" on page 193 of this chapter.

### Custom Reports

Custom Reports enable you to select the information you want to report on from all available report columns.

### Reports History

Contains a full history of generated reports maintained by 3Com Network Administrator. You can view old reports and export them to CSV using the Report History feature. To aid identification of old reports, the historical reports are tied to the currently loaded inventory.

### Export to CSV

You can export any generated report to CSV. This formatted text file can be imported into various applications, for example, Microsoft Excel. You can also use this feature to obtain a list of your network devices and properties to use in your own command line scripts.

## Components

This section describes the components of the Reporting feature.

3Com Network Administrator contains a large number of reports. Feature-based reports are covered elsewhere in this guide, please refer to Table 22 for further information. In addition to these the following reports are also available:

- Inventory Report
- Capacity Report
- Changes Report

Reports are produced in HTML and may also be exported to CSV.

*Reports use a simple form of sorting in that the first column is sorted alpha-numerically. This does mean, however, that IP addresses are ordered incorrectly. For example,* 10.0.0.1, 10.0.0.11, 10.0.0.12, 10.0.0.13 and so on.

### Inventory Report

You can obtain a report on the devices in the current inventory file using the Inventory report. For each device, the inventory report lists the following details:

- IP address
- Device type
- MAC address
- Device name

This report is launched from the *Reports* dialog and is selection-sensitive. If you have a number of devices in a stack (e.g. a Switch 3300 and 1100), all unit types are listed in the Type column. Similarly, if a modular device (e.g. the Switch 4007), has several blades in it, each blade type is listed in this column. For convenience, it also displays the number of devices at the start of the report.

## Capacity Report

The capacity report allows you to gauge how many available ports you have on your network. It lists the following details for each device:

- IP address
- Device type
- Total ports on the device
- Ports available (unused) on the device

This report provides information on all devices for which 3Com Network Administrator has port information.

At the bottom of the Ports available column is a summary listing the number of free ports across the device selection and a percentage of how many ports are available of the total ports present.

This report is launched from the *Reports* dialog and is selection-sensitive.

## Changes Report

This report is created during Refresh and gives information on device property changes, devices being added or removed from the network.

*The Changes report will not produce information on IP address changes to avoid large reports being generated on networks using DHCP.*

### Device Property Changes

This table details property changes for devices on the network. The device property changes reported on are:

- SNMP sysName
- SNMP sysDescr

The following unit changes are also reported:

- Unit added
- Unit removed
- Unit changed (a change of MAC address)
- Unit type changed
- Agent version changed

### VLAN Changes

VLAN changes are reported against each applicable device. A device can have any number of VLANs added, VLANs changed and VLANs removed tables.

*For the Switch 4007, a VLAN may be matched by its VLAN ID and the unit the VLAN is defined on. See "VLANS and the Switch 4007" on page 207 for further information.*

The VLAN details listed in this report section are:

- VLAN name
- VLAN unit (Switch 4007 only)
- VLAN ID
- Protocol information (if present)

The information is followed by a table of member ports, broken into untagged and tagged columns. The formatting is slightly different between VLAN added/removed and VLAN changed. Here is an example of VLAN changed:

**VLAN changed**
Name: Default VLAN
ID:1

Details:

| Previous Inventory File | Current Inventory File |
|---|---|
| Name: Default VLAN<br>Layer 3 Details<br>IP: 140.204.232.117/255.255.255.128 | Name: VLAN 5<br>Layer 3 Details<br>IP: 140.204.232.117/255.255.255.128 |

Ports:

| Previous Inventory File | Current Inventory File |
|---|---|
| Untagged ports:<br>Unit 1: 1, Ports 3-5, 7-24<br>Tagged ports:<br>Unit 1: Port 6 | Untagged ports:<br>Unit 1: Ports 1, 3-4, 7-24<br>Tagged ports:<br>Unit 1: Ports 5-6 |

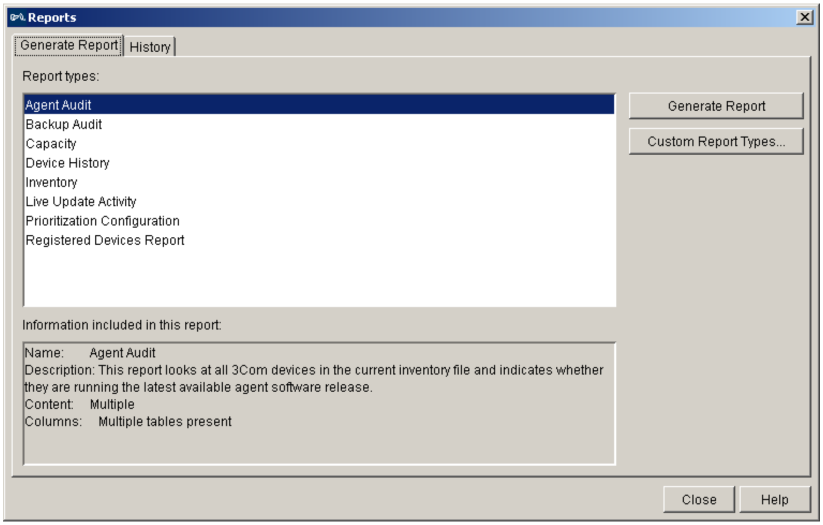
In the Ports table, untagged ports and tagged ports are always listed. If there are no untagged/tagged ports, then *None* is shown instead of the ports.

*For VLAN changed sections, if there are no changes to the member ports, the Ports table is not shown. Likewise, if there are no changes in the VLAN details, the VLAN details table is not shown.*

## Reports Dialog

The *Reports* dialog displays all the reports that you can generate using 3Com Network Administrator as shown in Figure 89:

**Figure 89** Reports Dialog



Agent Audit
Backup Audit
Capacity
Device History
Inventory
Live Update Activity
Prioritization Configuration
Registered Devices Report

Name: Agent Audit
Description: This report looks at all 3Com devices in the current inventory file and indicates whether they are running the latest available agent software release.
Content: Multiple
Columns: Multiple tables present

### Generate Report Tab

From the *Generate Report* tab you can select any report in the list. Clicking on a report will update the information presented in the text panel, under the label *Information included in this report*. This panel displays the following:

- **Name**
- **Description**
- **Content** — describes what the report will present. This is devices or ‘Multiple’ (which means that the report has multiple tables or components in it so its content cannot be summarized).
- **Columns** — lists the columns present in the table in this report. If the report has multiple tables, the value for columns will be ‘Multiple’.

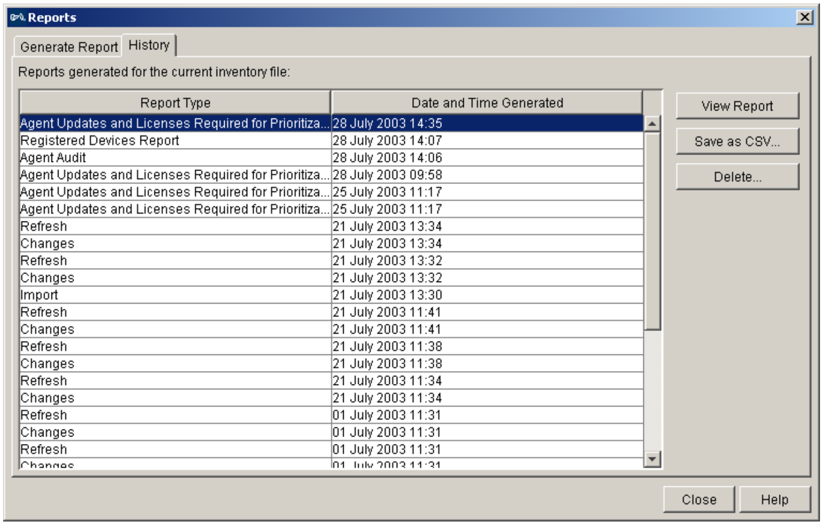
Click *Generate Report* to create the report you have selected in the Reports list. This will produce the report and open it in your default web browser. If you have some items selected, you will be presented with a dialog asking if you wish to produce a report for all items in the current inventory file. The default is 'Yes'. If you answer 'No', the report will be produced based on the current selection. If *Generate Report* is clicked when there is no selection, the report is automatically produced on all items in the current inventory file. See "'Generate Report' not Working" on page 208 if you have problems generating a report.

*Custom Report Types* launches a dialog where you can add, edit and delete custom/user-defined reports. See "Custom Report Types Dialog" on page 200 for more information.

### History Tab

The History tab of the *Reports* dialog allows you to view previously generated reports as shown in Figure 90:

**Figure 90** History Tab



Reports generated for the current inventory file:

| Report Type | Date and Time Generated |
|---|---|
| Agent Updates and Licenses Required for Prioritiza... | 28 July 2003 14:35 |
| Registered Devices Report | 28 July 2003 14:07 |
| Agent Audit | 28 July 2003 14:06 |
| Agent Updates and Licenses Required for Prioritiza... | 28 July 2003 09:58 |
| Agent Updates and Licenses Required for Prioritiza... | 25 July 2003 11:17 |
| Agent Updates and Licenses Required for Prioritiza... | 25 July 2003 11:17 |
| Refresh | 21 July 2003 13:34 |
| Changes | 21 July 2003 13:34 |
| Refresh | 21 July 2003 13:32 |
| Changes | 21 July 2003 13:32 |
| Import | 21 July 2003 13:30 |
| Refresh | 21 July 2003 11:41 |
| Changes | 21 July 2003 11:41 |
| Refresh | 21 July 2003 11:38 |
| Changes | 21 July 2003 11:38 |
| Refresh | 21 July 2003 11:34 |
| Changes | 21 July 2003 11:34 |
| Refresh | 01 July 2003 11:31 |
| Changes | 01 July 2003 11:31 |
| Refresh | 01 July 2003 11:31 |
| Changes | 01 July 2003 11:31 |

The following options are available:

- **View Report** — click this button to launch the selected report in your default web browser.

- **Save as CSV** — click this button to display a standard file chooser dialog prompting you for a file location to save the current selected report in CSV form.

  The CSV format used for exported reports is:

  ```
  <Report title>

  <Table title>

  <Table Heading 1>, <Table Heading2>, ...

  <Row 1 Column 1>, <Row 1 Column 2>, ...
  <Row 2 Column 1>, <Row 2 Column 2>, ...
  ```

For example:

```
Misconfiguration and Optimizations Report

Misconfigured Link

End1, End 2
Switch1100-1 (Unit 1 Port 1), Switch1100-2 (Unit 1 Port
2)s
Switch3300-1 (Unit 2 Port 1), Switch3300-2 (Unit 1 Port 5)
```

*Blocks of text (e.g. report description, table descriptions etc.) will **not** appear in the CSV file.*

- **Delete** — click this button to display a dialog asking for delete confirmation before the generated report is removed from the disk and this table.

*See "Disk Usage" on page 207 for information on disk space usage by the Reports feature.*

The table of reports can be sorted by clicking on the column headers. This is useful when trying to find a particular report to view or to aid deletion of old reports, for example. It lists any reports that have been generated since the current inventory file has been opened or created. It does not include reports generated against other inventory files.

*Any reports that are created against an untitled or new inventory file are lost if that inventory file is not saved before closing it.*

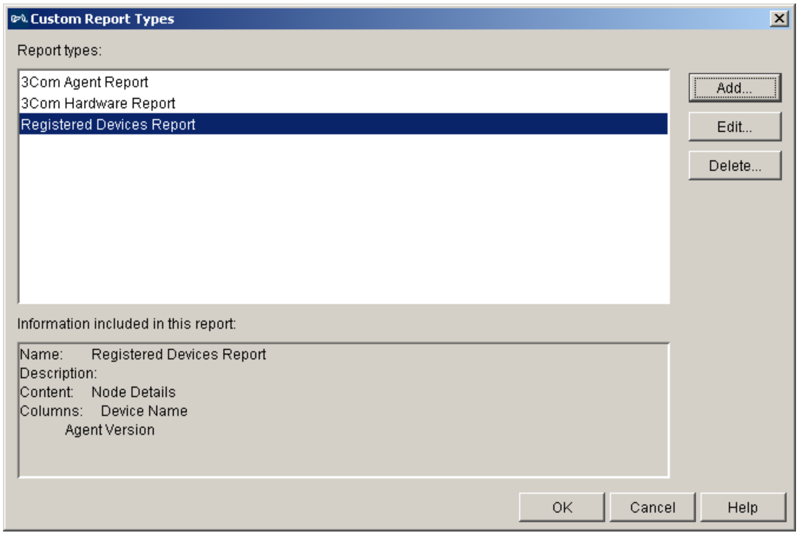
## Custom Report Types Dialog

The *Custom Report Types* dialog enables you to:

- Create new custom reports
- Edit existing custom reports
- Delete custom reports

The list shown in Figure 91, displays any custom reports already created. It does **not** list any of the pre-defined reports.

**Figure 91** Custom Report Types



3Com Agent Report
3Com Hardware Report
Registered Devices Report

Name: Registered Devices Report
Description:
Content: Node Details
Columns: Device Name
Agent Version

The panel in this dialog entitled *Information included in this report* works in the same way as the panel in the main reports dialog.

*If you edit an existing report, you are warned that if you change the columns used in the report then 3Com Network Administrator will remove any existing reports (i.e. the reports in the history tabbed pane of the* Main Reports *dialog) that were generated from that report type. However, if you edit the report and only change the description (i.e. you do not change the columns), all generated reports for that report* ***will*** *be preserved. If you then click* View Report *for one of these generated reports (or Save to CSV) the new description will be used.*

## Add/Edit Report Wizard

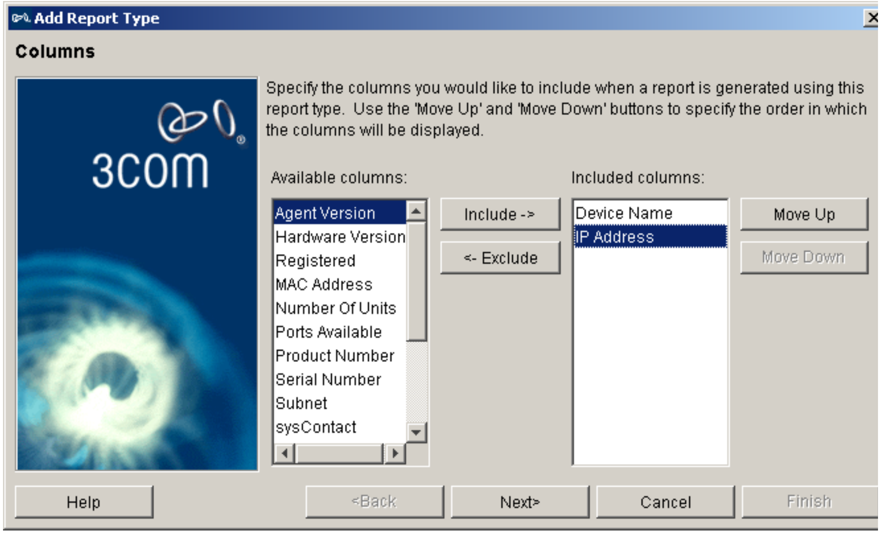
From the Add/Edit Report Wizard you can add and amend reports that detail information about the 3Com devices on your network.

*The Add/Edit Report Wizard can be launched from the* Custom Report Types *dialog.*

### Columns Step

The *Columns* step is the first step in the wizard as shown in Figure 92:

**Figure 92** Add/Edit Report Wizard - Columns Step



Add Report Type

Columns

Specify the columns you would like to include when a report is generated using this report type. Use the 'Move Up' and 'Move Down' buttons to specify the order in which the columns will be displayed.

There are two lists as follows:

- **Available columns —** lists columns that can be included in the report. Select a column from the list and click *Include* - > to add the column to the report.
- **Included columns** — lists columns included in the report. Included columns will be used to compose a table for the Custom report and will be ordered from left to right as the list is ordered from top to bottom. For example, in Figure 92, *Device Name* will be the first column in the report. To remove a column from the report, select the column and click < - *Exclude*.

Once columns are included in a report, you can change the order the columns appear in by selecting an entry in the included columns and clicking *Move Up* or *Move Down* to change their position in the table. The first entry in the list appears in the first column of the table and so on.

*The first column is used to sort the entire report so if you wish to sort the report by device name, for example, then ensure the* Device Name *column is first in the report.*

Table 23 shows the available columns:

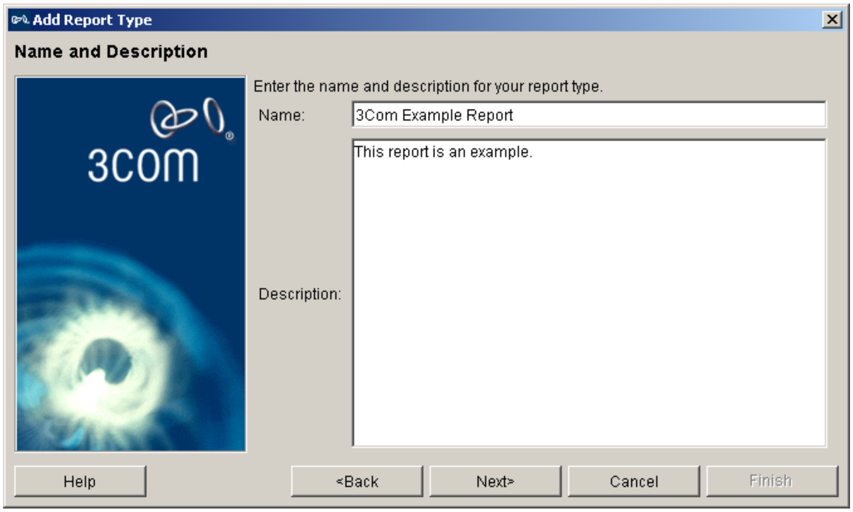
**Table 23** Available Columns

| **Column** | **Description** |
|---|---|
| Agent Version | The software agent version running on a device e.g. 3.0.0. If the agent version is not available then *N/A* is displayed in this column. |
| Device Name | The name of the device, which is one of the following: custom name, DNS name, SNMP sysName, IP address, MAC address. |
| IP Address | The IP address of the device, or *Unknown* if it is not known. |
| MAC Address | The MAC address or addresses associated with a device. |
| Number of Units | The number of units a device consists of, i.e. the number of cards in a modular system or the number of units in a stack. |
| Ports Available | The number of ports on a device. |
| Registered | Whether the device has been registered with 3Com using the Device Warranty feature. |
| Subnet | The subnet the device is on, e.g. 104.204.1.0 (255.255.255.0) |
| sysDescr | The value of SNMP object sysDescr for the device. |
| sysName | The value of SNMP object sysName for the device. |
| sysOid | The value of SNMP object sysOid for the device. |
| Total Ports | The total number of ports on a device. |
| Type | The type of the device e.g. ‘3Com Switch 3300’ |
| Used Ports | The number of used ports on a device. |

### Name and Description Step

You can use this step to specify the name and description of your custom report as shown in Figure 93:

**Figure 93** Add/Edit Report Wizard - Name and Description Step



Enter the name and description for your report type.

Name: 3Com Example Report

Description: This report is an example.

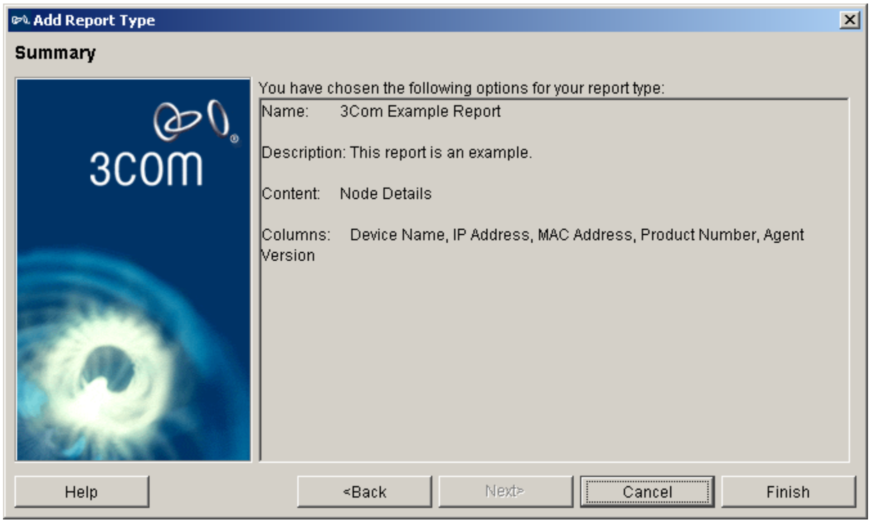
The name and description appears in the report when it is generated. They also display in the *Reports* dialog in the Report Information panel when this custom report is selected.

*If you are editing an existing custom report you cannot change the report name.*

### Summary Step

The final step shows all the values you have chosen for your custom report as shown in Figure 94:

**Figure 94** Add/Edit Report Wizard - Summary Step



You have chosen the following options for your report type:

Name: 3Com Example Report

Description: This report is an example.

Content: Node Details

Columns: Device Name, IP Address, MAC Address, Product Number, Agent Version

Click *Finish*, to add the report to the *Custom Reports* dialog. Click *OK* to close the *Custom Reports* dialog. You can now use your custom report in the same way as any of the pre-defined reports.

## Examples

The following section gives some examples of how the Reporting feature can be used. The feature-specific reports are covered in the chapter for the relevant feature. See "Feature Reports" on page 192 for further details.

### Assessing Network Expansion Capability

You have a number of additional servers to add to your network and you want to find out if you have enough capacity in your network and to work out which 3Com devices to connect them to.

You can get an assessment of how much network capacity you have by charting available ports using the *Save to CSV* facility in Reports, in combination with an external CSV tool such as Microsoft Excel as follows:

**1** Launch the *Reports* dialog from *Tools* > *Reports* and select the *Capacity Report*.

**2** Click *Generate Report*.

**3** Select the *History* tab of the *Reports* dialog and select the generated report in the table.

**4** Click *Save to CSV* and choose a location for the CSV file.

**5** Open the saved file in Microsoft Excel.

**6** Select the *IP Address* column, by drag-clicking the cell entry with the column title *IP Address* all the way down to the end of the IP Address data.

**7** Holding down *CTRL*, do the same with the *Total Ports* and *Ports Available* columns.

**8** Select *Chart* from the *Insert* menu.

**9** Use the defaults of *Chart Type: Column* and *Subtype: Clustered Column* and click *Next*.

**10** Click *Next* on the Chart Source Data wizard step.

**11** Click on the *Titles* tab on this wizard step, enter *Network Capacity* as the chart title and click *Next*.

**12** Choose to *Place chart as new sheet* and click *Finish.*

This gives you a graph showing at a glance how many ports you have free across your range of 3Com devices and where the servers could be best connected. You can also use Excel’s sorting feature to sort the table data by *Ports Available*, for example.

## Ensuring Stacks are Running the Same Agent Version

3Com recommends that all units in a stack are running the same agent version to avoid performance issues. You can generate a report providing this information using the custom report feature as follows:

1. Launch the *Reports* dialog from *Tools* > *Reports*.
2. Click *Custom Type Reports*.
3. Click *Add* to create a new custom report.
4. Select the columns you wish to view in your custom report. *Device name* is already an included column. Select any combination of the following columns and add them to the report:
   - Device type
   - IP address
   - Number of units
   - Agent version
5. Click *Next* and type *Agents on units* and provide a description.
6. Click *Next*.
7. After reviewing the details on the *Summary* step, click *Finish*.
8. Click *OK* in the *Custom Report Types* dialog to confirm the custom type addition.
9. Select *Agents on units* in the list of reports and click *Generate Report*.

   The report will enable you to see at a glance which stacks have more than one unit and what the unit agent versions are, allowing you to locate units that require agent version changes.

## Useful Information and References

The following section provides useful information and references when using Reports in 3Com Network Administrator.

### VLAN-unaware Devices

A VLAN-unaware device is:

- A device that does not support VLANs, or
- A device that supports VLANs but has no VLANs configured, or
- A device that supports VLANs, has exactly one VLAN configured and has all ports using untagged traffic for that VLAN. This enables 3Com Network Administrator to identify factory default switches with all ports on the 'default' VLAN.

### VLANS and the Switch 4007

The configuration of VLANs on the Switch 4007 differs from that on other device types. On the 4007, VLANs are created on each individual module in the chassis, i.e. VLANs cannot be created device-wide as with stackable devices. In order for a VLAN to span modules, the backplane ports of the modules must be members of the VLAN. However, if the backplane ports of a module are not members of a VLAN, this VLAN is effectively local to this module. Another completely separate VLAN can be defined on another module with the same VLAN ID.

## Key Considerations

The following section provides some useful advice when using the Reports feature in 3Com Network Administrator.

### Report Information Out-of-Date

The information that appears in Reports is based on information held in the current inventory file. If changes have occurred since the last refresh operation, the report will contain out-of-date information. The one exception to this is the Prioritization Configuration report, which uses SNMP queries on your network devices to generate this report.

### Disk Usage

Generated reports are not aged or deleted automatically in any way. Therefore, over a period of time, the number of reports stored on disk will build up. One generated report will take up approximately 4K to 5K, depending on the number of devices reported on. You can delete generated reports from the *Reports* > *History* tab.

If you have more than 500 generated reports stored, 3Com Network Administrator will display a warning when you launch the *Reports* dialog. This is purely informational and will not affect the operation of 3Com Network Administrator in any way.

When you generate a report, the report history is stored in XML format on disk. The HTML file produced is a temporary file that is removed once 3Com Network Administrator shuts down. If you wish to view an old report, you can use the Report History feature to view it. If you wish to use the HTML report outside of 3Com Network Administrator, generate the report and select *File > Save As* from your web browser to save the report to a location of your choice.

### 'Generate Report' not Working

Sometimes, when you click *Generate Report* in the *Reports* dialog it can seem as if nothing is happening. This may be because the inventory file is unusually large and therefore the report is taking a long time to generate.

# 10 HP OpenView Integration

## Overview

This chapter describes how 3Com Network Administrator integrates with HP OpenView.

Once 3Com Network Administrator has been installed you will find that when you next launch HP OpenView it has been customized for enhanced support of 3Com devices and 3Com management applications. Specifically the enhancements are as follows:

- Symbol customization for 3Com devices — HP OpenView will recognize 3Com devices and correctly identify their type. If you view the properties for a 3Com symbol on the map it will show the device type and the fact that it is a 3Com Connector.
- 3Com proprietary MIBs — you can use the HP OpenView MIB browser to access 3Com proprietary MIBs.
- Enhanced 3Com Trap Decoding — if HP OpenView receives a trap from a 3Com device it will display a more meaningful message in the alarm list.
- Menu customization for launching 3Com management applications.
- When a 3Com device is selected and if the device supports it, the following applications can be launched from the right-click menu:
  - **3Com Device View** — a 3Com device management application (only available for certain 3Com device types).
  - **3Com Web Interface** — if the 3Com device supports Web management this will launch the default Web browser against the selected device.
  - **3Com Switch Manager** — the element manager for the Switch 7700.
  - **3Com Router Manager** — the element manager for the 3Com router family.

- From the main *Tools* menu, there is an option to launch 3Com Network Administrator.
- From the *Help* menu, there is an option to view the 3Com Integration Kit Online manual.

This chapter covers the following topics:

## Key Concepts

The following section describes the key concepts of the HP OpenView Integration using 3Com Network Administrator.

### Alarms

3Com Network Administrator uses the HP OpenView Alarms list to report the results of certain administration operations that it performs. The operations that result in alarms being sent to HP OpenView are:

- Device Backup
- Device Restore
- Device Setup
- Agent Update

*The HP OpenView services need to be running for the alarm to be added to the list.*

For each of the above operations, 3Com Network Administrator generates a report that includes a summary of the status of the operation. The report will contain more detailed information than is presented in the HP OpenView alarm message. To view the report from 3Com Network Administrator select *Tools* > *Reports* > *History* tab.

### Getting Information from HP OpenView into 3Com Network Administrator

3Com devices that you have discovered using HP OpenView can be imported into the current 3Com Network Administrator inventory file. This enables you to use the 3Com-specific administration tools that 3Com Network Administrator provides on those devices.

*3Com Network Administrator imports 3Com devices from the database your HP OpenView installation is connected to.*

*More information on how to use the 3Com Network Administrator Import tool is available in* Chapter 5, "Importing and Refreshing Devices".

### Icons

The 3Com HP OpenView Integration Kit customizes the HP OpenView representation of 3Com devices, by providing customized icons. This enables you to identify your 3Com devices more easily on the HP OpenView map. Also, the integration customizes the HP OpenView database, which enables you to search for 3Com devices using HP OpenView's *Find* facility. All the 3Com symbol types will be added to the HP OpenView database and all 3Com devices will have the *is3ComConnector* attribute set.

To search for a specific 3Com device type on your HP OpenView map:

1. Select *Edit* > *Find* > *Object By Symbol Type* to launch the *Find By Type* dialog.
2. Select the *Connector* type in the first list box and then select the 3Com device type in the second list box.
3. Click *Apply* to display all the devices of that type.

To find all 3Com devices on your HP OpenView map:

1. Select *Edit* > *Find* > *Object By Attribute* to launch the *Find By Attribute* dialog.
2. Select the *is3ComConnector* attribute in the first list box.
3. Click *Apply* to display all the 3Com devices.

## MIBs

The Integration Kit also provides 3Com MIBs that can be accessed using the HP OpenView MIB browser. This gives you access to the low level configuration and information settings of your 3Com devices. This low level configuration is typically not available from 3Com Network Administrator.

The MIBs provided in the 3Com HP OpenView Integration kit also include the 3Com-specific traps that 3Com devices can send. You can view the traps added to HP OpenView by the integration kit as follows:

1. Select *Options* > *Event Configuration* to display the Event Configuration window.
2. In the upper list box, select *3Com Enterprise*. All 3Com enterprise-specific traps will be displayed in the lower list box.
3. Double-click on one of the traps in the lower list box to launch the *Modify Events* dialog. This allows you to view the trap description and modify the event message, should you so wish.

## Components

This section describes the 3Com-specific features that the HP OpenView Integration Kit adds to your copy of HP OpenView.

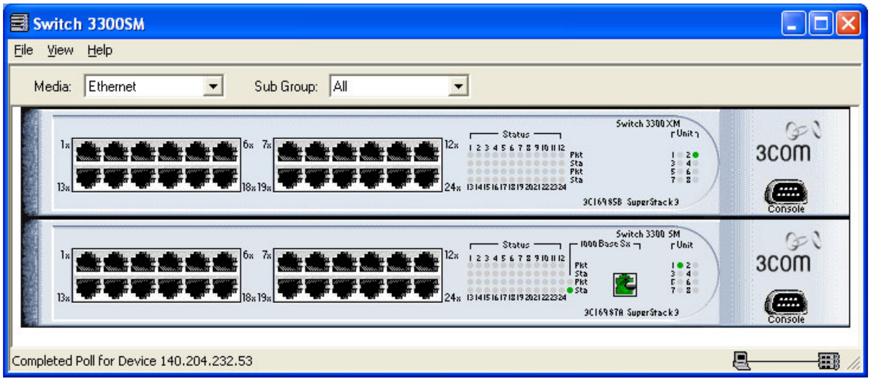
### Menu Components

The additional menu options provided by the 3Com HP OpenView Integration Kit are:

#### Device Menu

- **3Com Device View** — right-click on a device and select *Device View* to launch the 3Com Device View device management application, which provides a graphical view of the device and allows comprehensive configuration of certain parameters as shown in Figure 95.

**Figure 95** 3Com Device View



Media: Ethernet

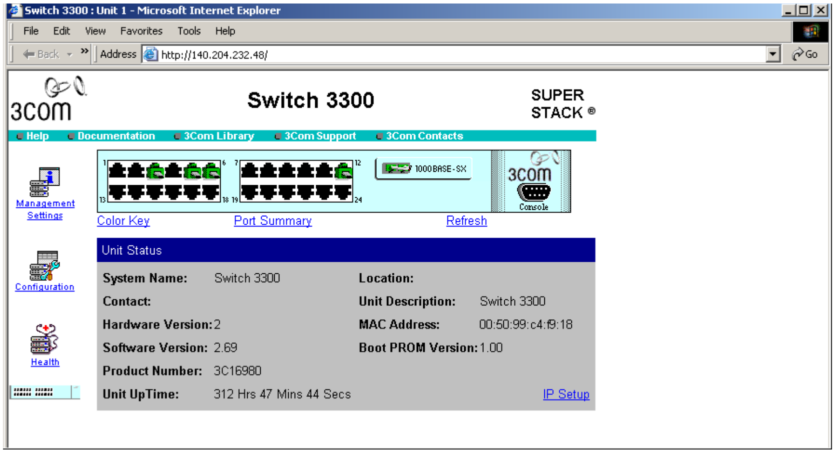
Sub Group: All

Completed Poll for Device 140.204.232.53

The menu option will only be available if 3Com Device View is supported by the selected device.

- **3Com Web Interface** — right-click on the device and select *Web Management* to launch your default Web browser to create a Web interface session with the selected device. This provides a graphical view of the device and allows access to many configurable parameters, as shown in Figure 96.

**Figure 96** 3Com Web Interface



Switch 3300 : Unit 1 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address http://140.204.232.48/
Go
3com
Switch 3300
SUPER STACK ®
Help Documentation 3Com Library 3Com Support 3Com Contacts
1000BASE-SX
Console
Management Settings
Configuration
Health
Color Key
Port Summary
Refresh
IP Setup

Unit Status

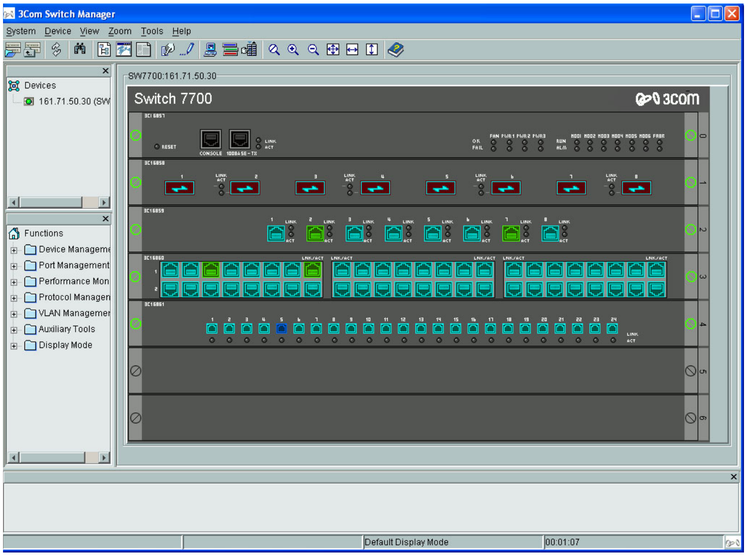
System Name: Switch 3300
Location:
Contact:
Unit Description: Switch 3300
Hardware Version: 2
MAC Address: 00:50:99:c4:f9:18
Software Version: 2.69
Boot PROM Version: 1.00
Product Number: 3C16980
Unit UpTime: 312 Hrs 47 Mins 44 Secs

The menu option will only be available if the selected device supports Web management.

## 3Com Switch Manager

Right-click on the device and select *Switch Manager* to launch the switch management application for the Switch 7700 as shown in Figure 97.

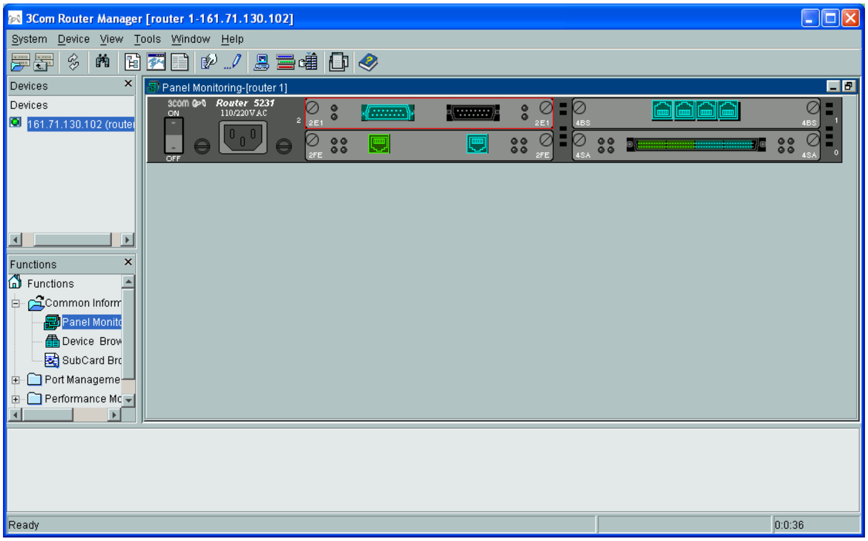
**Figure 97** 3Com Switch Manager



## 3Com Router Manager

Right-click on the device and select *Router Manager* to launch the router management application for the selected device as shown in Figure 98:

**Figure 98** 3Com Router Manager



## Tools > 3Com Network Administrator

This launches the 3Com Network Administrator application. It has the same effect as launching the application from the Windows Start menu.

## Help > 3Com Integration Kit Online Manual

This launches your default Web browser to display the online manual for the integration kit.

## Application Index Dialog

For each 3Com application that the 3Com HP OpenView Integration Kit installs, an entry will appear in the HP OpenView Application list. An index of all installed HP OpenView applications can be viewed as follows:

1 Select *Help > About HP OpenView...* to launch the *About HP OpenView* dialog.

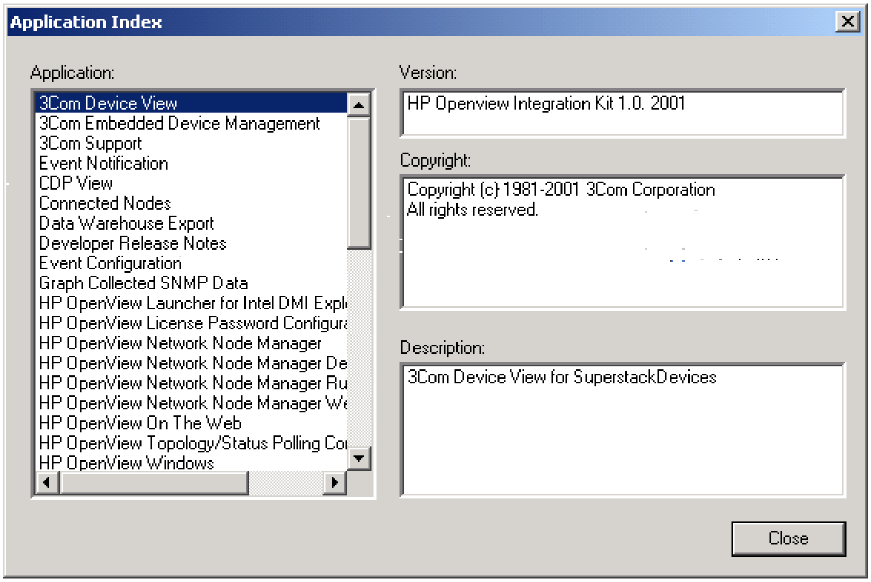
2 Click *Applications* on the dialog to launch the *Application Index* dialog.

**3** All the installed 3Com applications will appear, in alphabetical order, in the list box, as shown in Figure 99. The possible options include:

- 3Com Network Administrator
- 3Com Device View
- 3Com Embedded Device Management
- 3Com Switch Manager
- 3Com Router Manager
- 3Com HP OpenView Integration Kit

Select an application from the Application list to view detailed information about it, for example, Version, Copyright and Description, as shown in Figure 99.

**Figure 99** HP OpenView Application Index Dialog



Application Index

Application:

3Com Device View
3Com Embedded Device Management
3Com Support
Event Notification
CDP View
Connected Nodes
Data Warehouse Export
Developer Release Notes
Event Configuration
Graph Collected SNMP Data
HP OpenView Launcher for Intel DMI Expl
HP OpenView License Password Configur
HP OpenView Network Node Manager
HP OpenView Network Node Manager De
HP OpenView Network Node Manager Ru
HP OpenView Network Node Manager W
HP OpenView On The Web
HP OpenView Topology/Status Polling Co
HP OpenView Windows

Version: HP Openview Integration Kit 1.0. 2001

Copyright: Copyright (c) 1981-2001 3Com Corporation
All rights reserved.

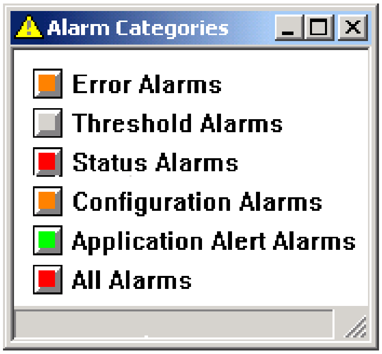
Description: 3Com Device View for SuperstackDevices

*You will need to quote the version number when talking to a 3Com Technical Support representative.*

### Alarm Categories

The Application Alert Alarms Category (as shown in Figure 100) is used by 3Com Network Administrator to provide the status of any Backup, Restore, Setup and Agent Update operations.

**Figure 100** HP OpenView Alarm Categories List



- 🟧 Error Alarms
- ⬜ Threshold Alarms
- 🟥 Status Alarms
- 🟧 Configuration Alarms
- 🟩 Application Alert Alarms
- 🟥 All Alarms

## Examples

This section describes some configuration examples using the HP OpenView Integration Kit.

### Launching 3Com Network Administrator from HP OpenView

In order to launch 3Com Network Administrator from HP OpenView, ensure that HP OpenView is already running and proceed as follows:

1. Select *Tools* > *3Com Network Administrator.*
2. The 3Com Network Administrator *Welcome* dialog displays, followed by the device window.

   You can now work with an inventory file that you previously created or create a new inventory file and import devices from HP OpenView. See "Importing from HP OpenView" in Chapter 5 for more information.

### Importing Device Information from HP OpenView

To create a new 3Com Network Administrator inventory file, containing devices from one of your HP OpenView subnets, do the following:

1. When the 3Com Network Administrator *Welcome* dialog appears, choose *Create a new inventory file*.
2. Launch the *Import* dialog by selecting the *File* > *Import* menu.

3 Ensure that the *Import From HP OpenView* radio button is selected (it is selected by default) and click *OK*.

4 A list of subnets displays. Select the subnet you require and click *OK*.

5 The *Import Progress* dialog displays indicating that it is importing the devices on your selected subnet. After a while the *Import Progress* dialog will close and be replaced by the *Refresh Progress* dialog listing the existing devices in the subnet.

6 When the refresh completes, the *Summary* dialog displays and should indicate that there were no import or refresh problems. If there are any, try to resolve them. For further information on how to do this see "Importing and Refreshing Devices" on page 87.

7 Close the *Summary* dialog and the new devices are added to the inventory. Confirm this by selecting the relevant subnet in the tree. The devices appear in the device list shown in the device window.

8 You can now use the configuration tools that 3Com Network Administrator provides to manage the new devices.

## Using the HP OpenView MIB browser

MIBs contain low-level information such as detailed statistical data and the RMON counters. Using a MIB browser to access this low-level information is for advanced users only, however it does allow greater control of your network. For example, you can use the HP OpenView MIB browser to view the security settings on all ports of one of your 3Com devices.

1 Select the device you are interested in on the HP OpenView map.

2 Select *Tools > SNMP MIB Browser.*

3 Navigate the MIB tree and select the branch:

```
iso.org.dod.internet.private.enterprises.a3Com.generic.secur
ePort
```

4 Click *Start Query*. After a short while the list box will be populated with all the entries in this table.

*You can obtain descriptions of each column in the table by expanding the tree to show all the table columns, selecting the column you are interested in, and then selecting* Describe*.*

## Key Considerations

The following section provides useful information and advice on the HP OpenView Integration Kit.

### Alarms Sent

Alarms are sent from 3Com Network Administrator to HP OpenView as shown in Table 24:

**Table 24** Alarm Information

| Alarm | Description |
|---|---|
| ■ Device Backup Success | For every successful device backup, restore, step and agent update, an alarm is sent to HP OpenView. Additional information about the backup operation is included in the alarm message field. |
| ■ Device Restore Success | |
| ■ Device Setup Success | |
| ■ Agent Update Success | |
| ■ Device Backup Failure | For every device backup that fails, an alarm is sent to HP OpenView. The reason for the failure is included in the alarm message field. |
| ■ Device Restore Failure | |
| ■ Device Setup Failure | |
| ■ Agent Update Failure | |

*For further information on the information traps that are used in HP OpenView's alarm list see Appendix A on page 241.*

# 11 Live Update

## Overview

This chapter describes how you can use Live Update to download product updates and product news from 3Com over the Internet. Live Update checks the 3Com server for available software updates and filters the updates so that only files that apply will be downloaded. Live Update also manages the download of these files.

By downloading and installing 3Com Network Administrator updates, you can ensure that 3Com Network Administrator is up-to-date, enabling you to take advantage of the latest bug-fixes and device support.

The latest 3Com Product News notifies you of new 3Com products and also contains articles on how to make the most of the features on your existing devices.

The following topics are covered in this chapter:

- Key Concepts
- Components
- Examples
- Useful Information and References
- Key Considerations

## Key Concepts

This section describes the keys concepts of Live Update.

### Connection Type

3Com Network Administrator supports three methods of connecting to the Live Update server:

- **Use Browser Settings** — 3Com Network Administrator checks the settings of your default browser and uses the same settings to connect to the Internet.
- **Direct Connection to the Internet** — 3Com Network Administrator assumes it has a direct connection to the Internet.
- **Use Custom Proxy Settings** — you can specify the proxy settings that 3Com Network Administrator should use to connect to the Internet.

### Service Packs

A Service Pack is an installable software component that keeps 3Com Network Administrator up-to-date. It provides updates such as:

- Latest bug fixes.
- ‘Day-one’ management support for the latest 3Com devices.

### Live Update Engine

The Live Update engine ensures that you download only the updates that are relevant to you as follows:

- 3Com Network Administrator updates — the Live Update engine lists an update only if it is more recent than the version already installed on your PC.
- Latest 3Com Product News — the Live Update engine only downloads news that you have not already downloaded.

## Components

The following section describes the Live Update Components in 3Com Network Administrator.

Live Update can be launched by:

- Clicking *Live Update* on the toolbar.
- Selecting the *Tools* > *Live Update* menu option.

Live Update consists of two main components:

- The Live Update Setup Wizard — this lets you select the type of Internet connection.
- The Live Update dialog — this dialog lists the available updates and lets you choose the ones you want to download.

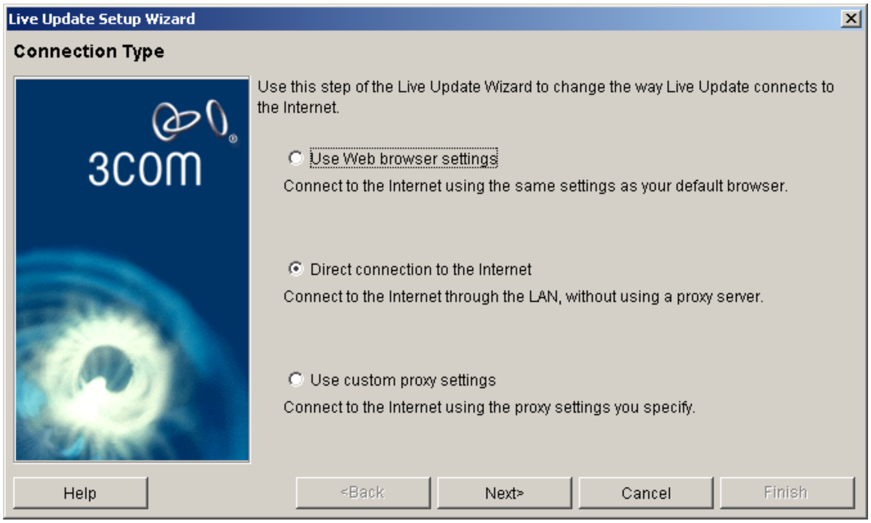
### Live Update Setup Wizard

The Live Update Setup Wizard is launched the first time you use Live Update. You can choose the way 3Com Network Administrator connects to the Internet and specify the proxy settings.

### Connection Type Step

From the *Connection Type* step you can select the preferred method to connect to the Internet as shown in Figure 101.

**Figure 101** Live Update Setup Wizard - Connection Type Step



Live Update Setup Wizard

Connection Type

Use this step of the Live Update Wizard to change the way Live Update connects to the Internet.

○ Use Web browser settings
Connect to the Internet using the same settings as your default browser.

● Direct connection to the Internet
Connect to the Internet through the LAN, without using a proxy server.

○ Use custom proxy settings
Connect to the Internet using the proxy settings you specify.

These are as follows:

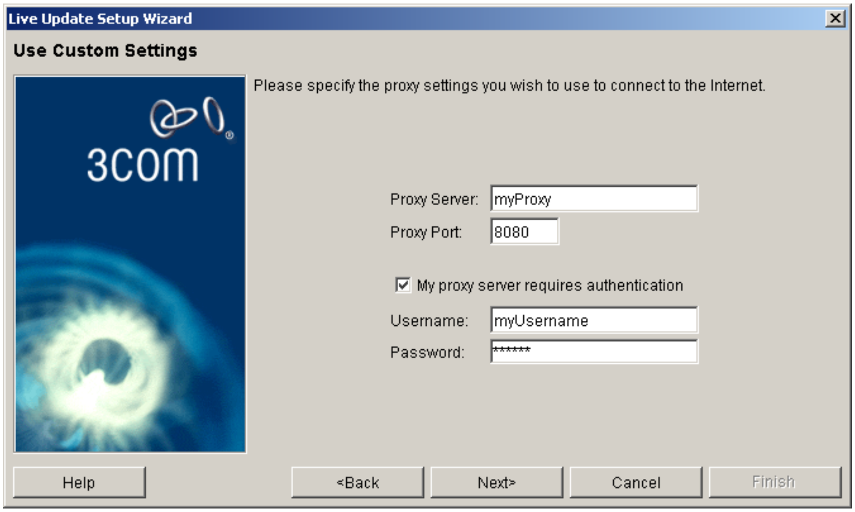
- **Use Web browser settings** — 3Com Network Administrator uses the same settings as your default browser to connect to the Internet. This is the recommended setting if the default browser on your PC is supported by 3Com Network Administrator.
- **Direct connection to the Internet** — 3Com Network Administrator connects directly to the Internet through the LAN.
- **Use custom proxy settings** — 3Com Network Administrator uses a proxy server that you specify to connect to the Internet. This is the recommended setting if you require a proxy server to connect to the Internet and your default browser is not configured to use that proxy or your default browser is not supported by 3Com Network Administrator. This is also recommended if your proxy server requires authentication (username and password).

*For more information on web browsers supported by 3Com Network Administrator see Appendix C on page 255.*

### Use Custom Settings Step

The *Use Custom Settings* step displays if you selected the *Use Custom Proxy Settings* option in the *Connection Type* step. From this step you can select the proxy settings such as a proxy server name, port, user name and password as shown in Figure 102.

**Figure 102** Live Update Setup Wizard - Use Custom Settings Step



Live Update Setup Wizard

Use Custom Settings

Please specify the proxy settings you wish to use to connect to the Internet.

Proxy Server: myProxy

Proxy Port: 8080

☑ My proxy server requires authentication

Username: myUsername

Password: ******

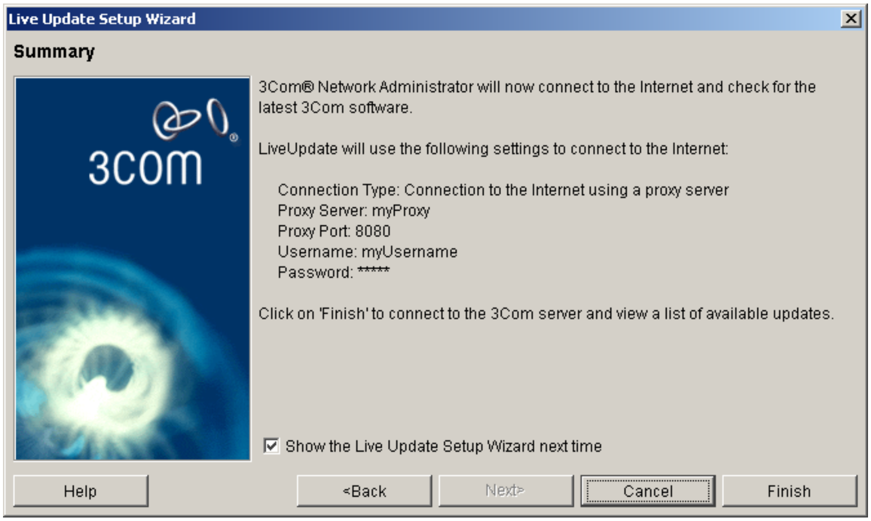
This step enables you to enter the following:

- **Proxy Server** — either the DNS name or the IP address of your proxy server.
- **Proxy Port** — the port number that 3Com Network Administrator should use to connect to your proxy server.
- **My proxy server requires authentication** — select this option if your proxy server requires authentication. If this option is not selected, the *Username* and *Password* fields will be ignored.
- **Username** — enter the username that 3Com Network Administrator should use to access the proxy server. This field can only be edited if the *My proxy server requires authentication* check box is selected.
- **Password** — enter the password that 3Com Network Administrator should use to access the proxy server. This field can only be edited if the *My proxy server requires authentication* check box is selected.

### Summary Step

The *Summary* step allows you to review the connection settings as shown in Figure 103.

**Figure 103** Live Update Setup Wizard - Summary Step



3Com® Network Administrator will now connect to the Internet and check for the latest 3Com software.

LiveUpdate will use the following settings to connect to the Internet:

Connection Type: Connection to the Internet using a proxy server
Proxy Server: myProxy
Proxy Port: 8080
Username: myUsername
Password: *****

Click on 'Finish' to connect to the 3Com server and view a list of available updates.

☑ Show the Live Update Setup Wizard next time

This step details the following:

- **Connection Type** — the type of connection that 3Com Network Administrator will use to connect to the Internet.
- **Proxy Server** — the name or IP address of the proxy server that 3Com Network Administrator will use to connect to the Internet. This information is displayed if you selected *Use Web browser settings* and your default browser is configured to use a proxy server to connect to the Internet or if you selected *Use custom proxy settings* in the *Connection Type* step.
- **Proxy Port** — the port that 3Com Network Administrator will connect to on the proxy server. This information is displayed if:
  - You selected *Use Web browser settings* and your default browser is configured to use a proxy server to connect to the Internet.
  - You selected *Use custom proxy settings* in the *Connection Type* step.
- **Username** — the username that 3Com Network Administrator will use to connect to the proxy server. This information is displayed only if you selected *Use custom proxy settings* in the *Connection Type* step and selected the *My proxy server requires authentication* check box in the *Use Custom Settings* step.
- **Password** — the password that 3Com Network Administrator will use to connect to the proxy server. This information is displayed only if you selected *Use custom proxy settings* in the *Connection Type* step and selected the *My proxy server requires authentication* check box in the *Use Custom Settings* step.
- **Show the Live Update Setup Wizard next time** — select this option if you want the Live Update Setup Wizard to be displayed the next time you run Live Update. De-select this option if you do not want this wizard to be displayed the next time you run Live Update.

Click *Finish* to connect to the Internet.

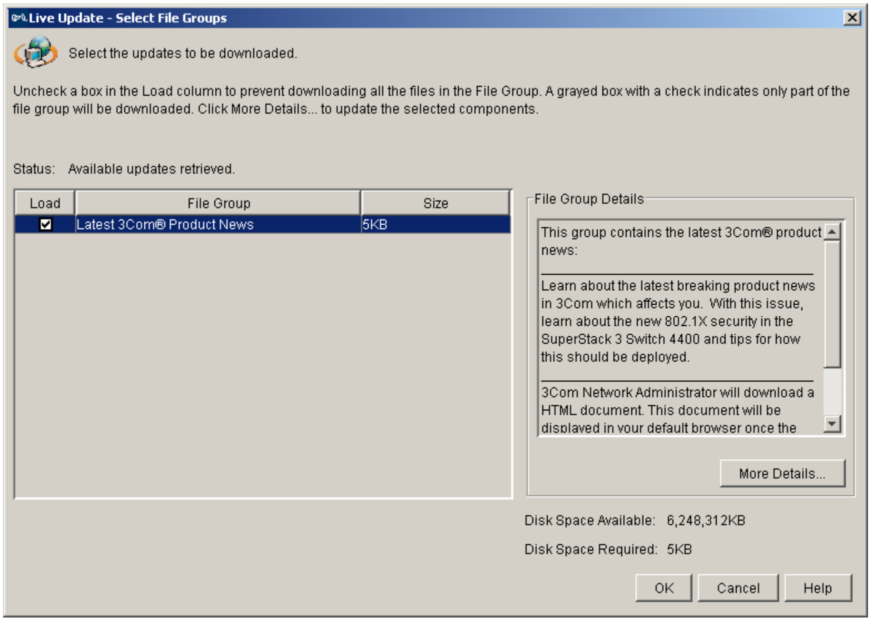
*If your proxy server requires authentication and you did not specify a username/password, you will be prompted to enter a username/password.*

*If your proxy server requires authentication and the username/password you provided have not been accepted, you will be prompted to enter a new username/password. If you no longer wish to connect to the Internet, click* Cancel.

## Live Update Select File Groups Dialog

The *Live Update - Select File Groups* dialog lists the types of updates that are available to download as shown in Figure 104.

**Figure 104** Live Update - Select File Groups



Select the updates to be downloaded.

Uncheck a box in the Load column to prevent downloading all the files in the File Group. A grayed box with a check indicates only part of the file group will be downloaded. Click More Details... to update the selected components.

Status: Available updates retrieved.

| Load | File Group | Size |
|---|---|---|
| ☑ | Latest 3Com® Product News | 5KB |

File Group Details

This group contains the latest 3Com® product news:

Learn about the latest breaking product news in 3Com which affects you. With this issue, learn about the new 802.1X security in the SuperStack 3 Switch 4400 and tips for how this should be deployed.

3Com Network Administrator will download a HTML document. This document will be displayed in your default browser once the

Disk Space Available: 6,248,312KB

Disk Space Required: 5KB

The dialog displays if:

- The *Show the Live Update Setup Wizard Next Time* option is selected in the *Summary* step of the Live Update Setup Wizard.
- The *Show the Live Update Setup Wizard Next Time* option is not selected in the *General* tab of the *Options* dialog but you have clicked on *Live Update* or selected the *Tools* > *Live Update* menu option.

### Status

This is the current status of the initial transaction between your PC and the Live Update server. The Status field will show one of the following:

- **Searching for available updates** — 3Com Network Administrator is connecting to the Live Update server and looking for the updates that are relevant to you.
- **Available updates retrieved** — 3Com Network Administrator completed the initial transaction with the Live Update Server. If any updates are available, they are displayed in the list underneath the status message.
- **Failed to retrieve update details** — the initial transaction between 3Com Network Administrator and the Live Update server failed. In this case, an error message is also displayed to help you identify the cause of the problem.

### Table of Available Updates

The table in the *Live Update - Select File Groups* dialog lists the types of update available for download. You can also select the file group that should be downloaded and the total space required on your PC.

The table consists of three columns as follows:

- **Load** — when this box is selected, all updates within the file group are selected for download. When this box is de-selected, all updates within the file group are excluded from the download. When this box is selected and greyed out, some updates within this file group are selected, whereas some are not. Click *More Details* to select/de-select individual files for download within that group. For more information see "Select File Group - Group Name" on page 229.
- **File Group** — this column indicates the type of file group available for download. 3Com Network Administrator supports two file groups:
  - 3Com Network Administrator/Update — this group contains the latest software updates for 3Com Network Administrator, this can be a Service Pack or a main release.
  - Latest 3Com Product News — this group contains the latest news about 3Com products and services.

- **Size —** the total size required to download the selected files in that file group. Click *More Details* to view which files are selected for download. For more information see "Select File Group - Group Name" on page 229.

### File Group Details

The File Group Details section displays a description of the updates available within the selected group.

To display the description, select the file group in the table.

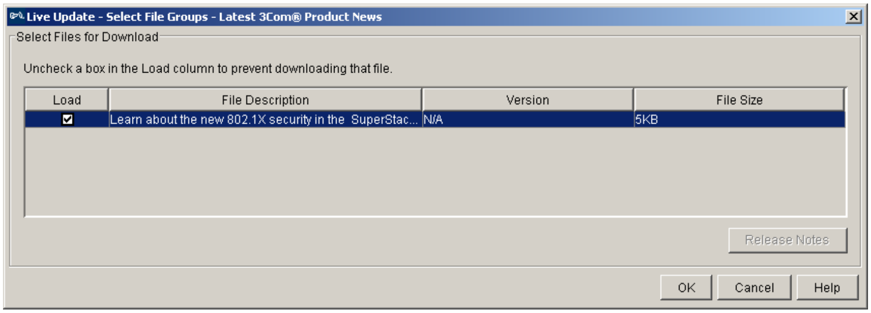
To view the contents of that file group in more detail, click *More Details*. For more information see "Select File Group - Group Name" on page 229.

## Select File Group - Group Name

This dialog displays the contents of the file group selected in the *Select File Groups* dialog as shown in Figure 105.

Use the check boxes in the *Load* column to select which files you want to download.

**Figure 105** Live Update - Select File Groups - Group Name



Live Update - Select File Groups - Latest 3Com® Product News

Select Files for Download

Uncheck a box in the Load column to prevent downloading that file.

| Load | File Description | Version | File Size |
|---|---|---|---|
| ☑ | Learn about the new 802.1X security in the  SuperStac... | N/A | 5KB |

The title of the dialog corresponds to the file group selected. For example, if the file group selected is *3Com Network Administrator Update*, the title of the dialog will be *Select File Group - 3Com Network Administrator Update*.

The table in this dialog displays the following columns:

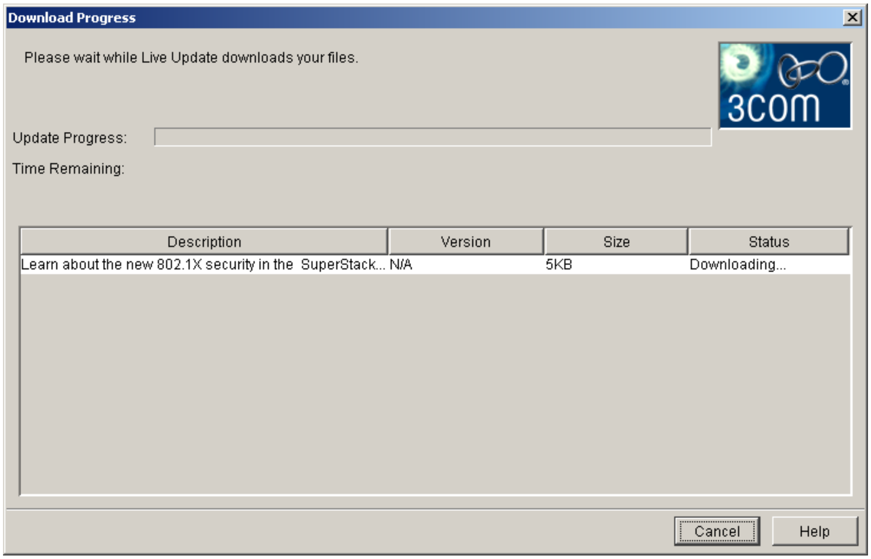
- **Load** — when this box is selected, the corresponding update is downloaded. De-select this box if you do not want to download this update.
- **File Description** — details of the downloadable file.
- **Version** — the value of this column depends on the file group as follows:
  - If the file group is *3Com Network Administrator Update,* this is the version of the update as well as the main version it applies to. For example, *SP1 (for 3NA v1.0)*.
  - If the file group is *Latest 3Com Product News* the version is not applicable (*N/A*).
- **File Size** — the size of the file(s) in KB.

The *Release Notes* button opens the release notes in Windows Notepad for the selected update. If no release note is available for the update, the *Release Notes* button will be greyed out.

## Download Progress

This dialog shows the progress of the ongoing download as shown in Figure 106.

**Figure 106** Download Progress



Download Progress

Please wait while Live Update downloads your files.

Update Progress:

Time Remaining:

| Description | Version | Size | Status |
|---|---|---|---|
| Learn about the new 802.1X security in the SuperStack... | N/A | 5KB | Downloading... |

This step details the following:

- **Update Progress** — this bar indicates the progress of the overall download.
- **Time Remaining** — this is an estimate of the time required to download all of the remaining files.
- **Table** — this indicates the download status of individual files (one of: *Pending..., Downloading..., Complete, Download Error*)

*If you click* Cancel *during the download, the download is suspended. If the connection is lost during the download or you clicked* Cancel *you can choose to resume the download or cancel it. The completed downloads remain on your PC.*

When the download is complete, the following occurs:

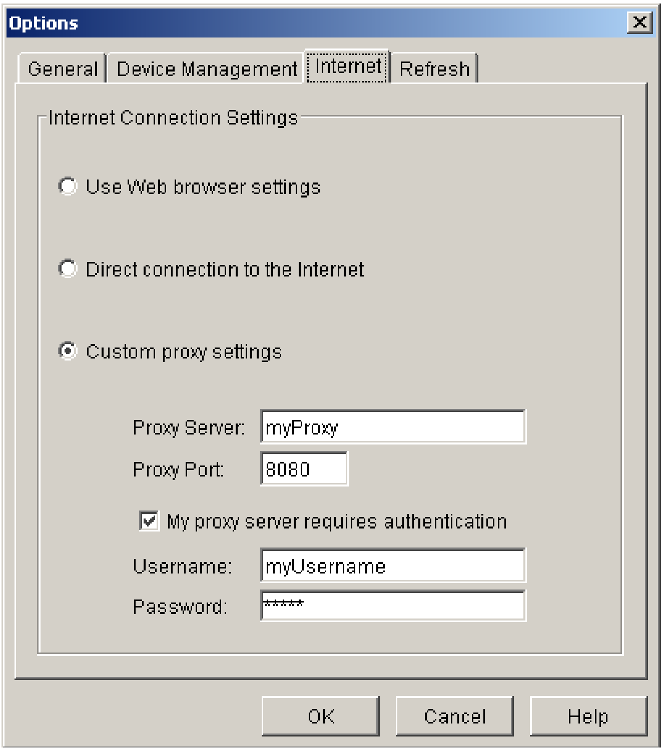
- If the update is the Latest 3Com Product News, the downloaded update is launched in your default browser.
- If the update is a 3Com Network Administrator update, you are required to restart 3Com Network Administrator. If you choose to restart, the update installs automatically. If you choose to restart later, the update installs the next time 3Com Network Administrator is launched.

*The 3Com Network Administrator update and the Latest 3Com Product News files are downloaded to the temporary folder on your PC (usually either* `C:\Temp` *or* `C:\Documents and Settings\My Profile\Local Settings\Temp`*).*

## Changing the Download Settings

The Internet tab in *Tools > Options* allows you to change the Internet connection settings as shown in Figure 107.

**Figure 107** Options - Internet



Internet Connection Settings

○ Use Web browser settings

○ Direct connection to the Internet

● Custom proxy settings

Proxy Server: myProxy

Proxy Port: 8080

☑ My proxy server requires authentication

Username: myUsername

Password: *****

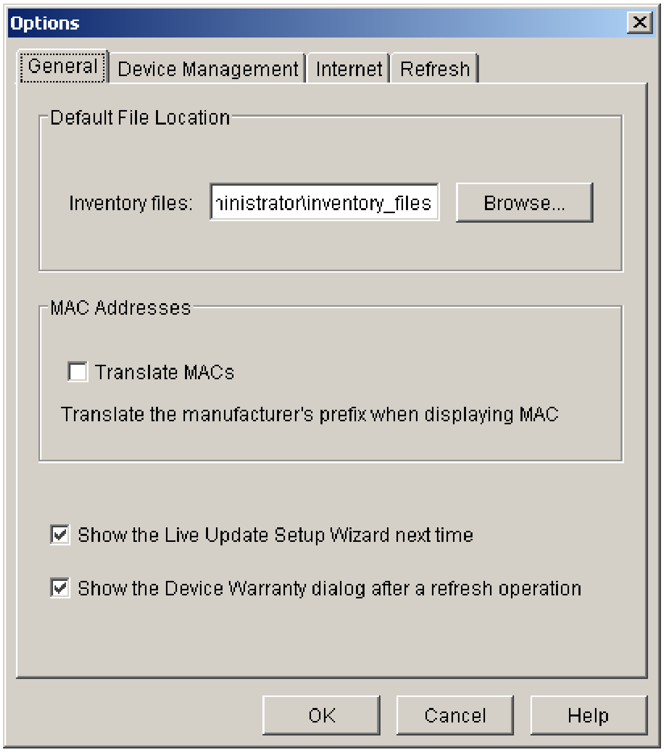
This tab contains the following:

- **Use Web browser settings** — 3Com Network Administrator uses the same settings as your default browser to connect to the Internet. This is the recommended setting if the default browser on your PC is supported by 3Com Network Administrator.
- **Direct connection to the Internet** — 3Com Network Administrator connects directly to the Internet through the LAN.
- **Custom proxy settings** — 3Com Network Administrator uses a proxy server that you specify to connect to the Internet. This is the recommended setting if you require a proxy server to connect to the Internet and your default browser is not configured to use that proxy, or your default browser is not supported by 3Com Network Administrator. This is also recommended if your proxy server requires authentication.

- **Proxy Server** — the name or IP address that 3Com Network Administrator uses to connect to the Internet. This field is only available when *Custom proxy settings* is selected.
- **Proxy Port** — the port that 3Com Network Administrator uses to connect to the proxy server. This field is only available when *Custom proxy settings* is selected.
- **My proxy server requires authentication** — select this option if your proxy server requires authentication.
- **Username** — the username that 3Com Network Administrator uses to access the proxy server. This field is only available when *Custom proxy settings* and the *My proxy server requires authentication* check box are selected.
- **Password** — the password that 3Com Network Administrator uses to access the proxy server. This field is only available when *Custom proxy settings* and the *My proxy server requires authentication* check box are selected.

The *General* tab in *Tools* > *Options*, allows you to choose whether the Live Update Setup Wizard should be displayed when you next run Live Update. Select the *Show the Live Update Setup Wizard next time* check box (as shown in Figure 108), to denote that the wizard should be displayed next time.

**Figure 108** Options - General



Options

Default File Location

Inventory files: ninistrator\inventory_files

MAC Addresses

☐ Translate MACs

Translate the manufacturer's prefix when displaying MAC

☑ Show the Live Update Setup Wizard next time

☑ Show the Device Warranty dialog after a refresh operation

## Live Update Activity Report

The Live Update Activity report can be used to review the download status of all the software updates downloaded using Live Update.

To view the report:

1. Select the *Tools > Reports* menu option.
2. In the *Generate Reports* tab, select the *Live Update Activity report*.
3. Click on *Generate Report.*

This will launch the Live Update Activity report in your default browser.

*If the download operation failed or was cancelled, the File Size column indicates 0 KB.*

## Examples

This section provides some examples of how to use Live Update.

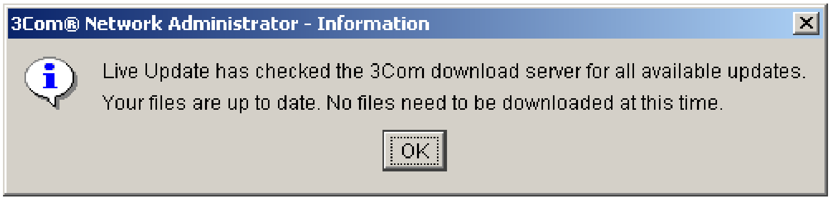
### Ensuring 3Com Devices are Supported

You have just bought some new hardware from 3Com and want to update your version of 3Com Network Administrator to ensure it supports these devices. To do this:

1. Click *Live Update* on the toolbar.
2. In the Live Update Setup Wizard, select *Use Browser Settings* and click *Next*.
3. Click *Finish*. 3Com Network Administrator will check for available software updates on the Live Update server.
4. The *Live Update - Select File Groups* dialog will display any available updates.

   If 3Com Network Administrator is up-to-date, you will get the message shown in Figure 109.

**Figure 109** 3Com Network Administrator Information Example

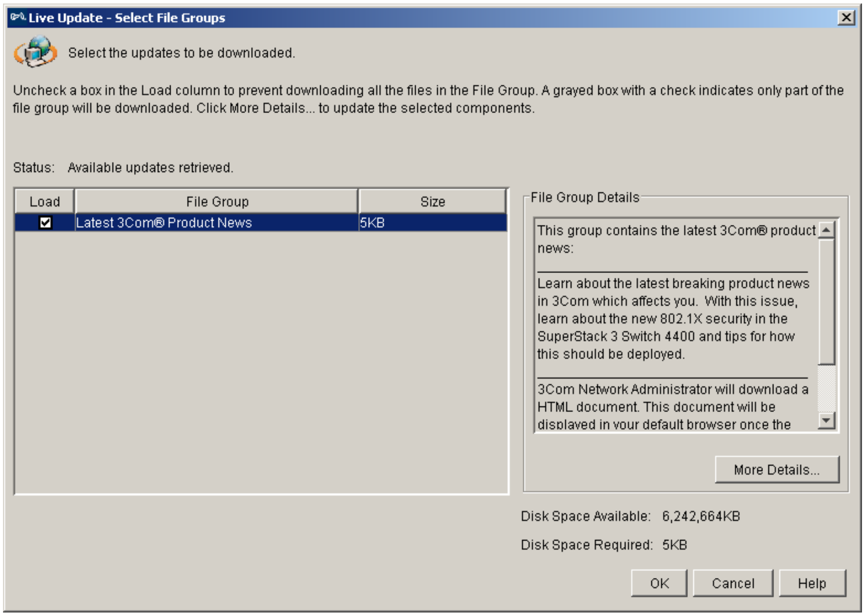


3Com® Network Administrator - Information

Live Update has checked the 3Com download server for all available updates. Your files are up to date. No files need to be downloaded at this time.

If an update is available, it will be listed in the dialog. The File Group Details tell you what benefits that update adds as shown in Figure 110.

**Figure 110** File Group Details Example



Live Update - Select File Groups

Select the updates to be downloaded.

Uncheck a box in the Load column to prevent downloading all the files in the File Group. A grayed box with a check indicates only part of the file group will be downloaded. Click More Details... to update the selected components.

Status: Available updates retrieved.

| Load | File Group | Size |
|---|---|---|
| ☑ | Latest 3Com® Product News | 5KB |

File Group Details

This group contains the latest 3Com® product news:

Learn about the latest breaking product news in 3Com which affects you. With this issue, learn about the new 802.1X security in the SuperStack 3 Switch 4400 and tips for how this should be deployed.

3Com Network Administrator will download a HTML document. This document will be displayed in your default browser once the

Disk Space Available: 6,242,664KB

Disk Space Required: 5KB

5 Click *More Details...* to view the details on that update. This will open the *Live Update - Select File Groups - 3Com Network Administrator Update* dialog.

6 Click *Release Notes* to display the readme file in Notepad. You can then check that this update adds support for your new 3Com devices.

7 Click *OK* to return to the *Live Update -Select File Groups* dialog.

8 Click *OK* to download the update.

9 When the download is complete you will be asked to restart 3Com Network Administrator. Click *Yes* to restart. The downloaded update will be installed automatically.

## Updating the Connection Information

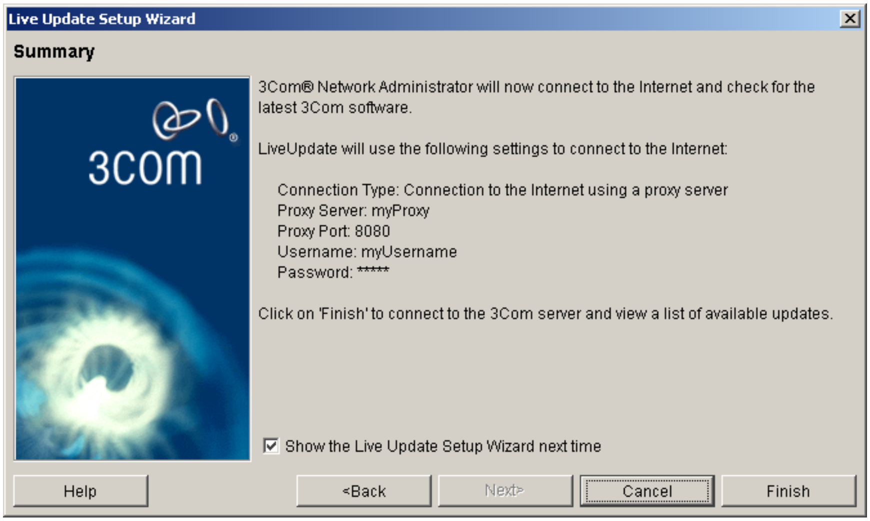
Your PC previously used a direct connection to the Internet, however, it now requires a proxy server. You want to update the Internet connection settings for Live Update.

### Solution 1 - Automatic Configuration using the Live Update Setup Wizard

This is the preferred method if your default browser is supported by 3Com Network Administrator and is configured to use the proxy server.

1. Select the *Tools* > *Options*... menu option.
2. Click the *General* tab.
3. Click *Show the Live Update Setup Wizard next time* option if it is not already selected.
4. Click *OK* to validate the changes.
5. Click *Live Update...*. This launches the Live Update Setup Wizard.
6. Select *Use Web Browser Settings* and click *Next*. The *Summary* dialog is displayed which shows the proxy settings that Live Update will now use (as shown in Figure 111).

**Figure 111** Automatic Configuration Example



3Com® Network Administrator will now connect to the Internet and check for the latest 3Com software.

LiveUpdate will use the following settings to connect to the Internet:

Connection Type: Connection to the Internet using a proxy server
Proxy Server: myProxy
Proxy Port: 8080
Username: myUsername
Password: *****

Click on 'Finish' to connect to the 3Com server and view a list of available updates.

☑ Show the Live Update Setup Wizard next time

7. Click *Finish* to connect to the Internet using the proxy server specified.

### Solution 2 - Manual Configuration Using the Options Dialog

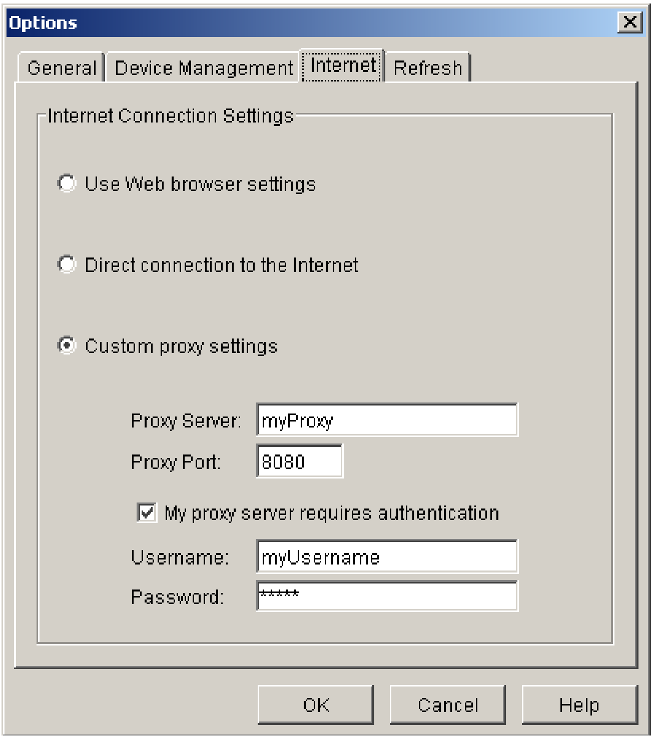
This is the preferred method if your default browser is not supported by 3Com Network Administrator or if your browser is not configured to use the proxy server.

1 Select the *Tools* > *Options*... menu option.

2 Click the *Internet* tab to display the Internet connections settings.

3 Select the *Custom Proxy Settings* option. You can now enter the proxy server name (or IP address) and the proxy port as shown in Figure 112:

**Figure 112** Tools - Options - Internet Tab Example



Options

General | Device Management | Internet | Refresh

Internet Connection Settings

○ Use Web browser settings

○ Direct connection to the Internet

● Custom proxy settings

Proxy Server: myProxy

Proxy Port: 8080

☑ My proxy server requires authentication

Username: myUsername

Password: *****

4 If your proxy server requires authentication, you can also enter a username and password in this dialog by selecting the *My proxy server requires authentication* check box.

5 Click *OK* to validate the changes.

## Useful Information and References

The following section provides useful details to do with Live Update.

### Proxy Server

A proxy server acts as an intermediary between the PCs on your network and the Internet.

The main features of a proxy server are:

- Centralized access to the Internet for all the PCs on your network.
- Web content filtering
- Internet access restricted to authorized users.

In most cases, proxy servers also support authentication (also known as *logging)* whereby the users must provide a username/password before connecting to the Internet. This ensures that only authorized personnel are able to access the Internet.

## Key Considerations

The following section provides assistance when using Live Update.

### The Proxy Settings are not Retrieved

A description of this problem is as follows:

- Your browser is using a proxy server to connect to the Internet.
- In the *Connection Settings* step of the Live Update Setup Wizard, you selected *Use Browser Settings*. However, in the *Summary* step of the Live Update Setup Wizard, the connection type is set to *Direct Connection to the Internet* when it should be *Connection to the Internet using a proxy server.*
- After clicking *Finish*, you get an error message. The most likely reason for this is that your browser is not supported by 3Com Network Administrator.

A suggested solution is as follows:

1. Open your browser and go to the Internet Connection Properties.
2. Write down the proxy server settings (proxy server name/IP address and proxy port). If available, also write down the username and password.
3. In 3Com Network Administrator, select *Tools* > *Options* and select the *Internet* tab.

4 Select the *Custom Proxy Settings* option and enter the proxy server name/IP address and the proxy port. If your proxy server requires authentication, select the *My proxy server requires authentication* check box and enter the username and password.

5 Click *OK* to validate the settings.

6 Launch the Live Update Setup Wizard and proceed to the *Summary* step (which should now show the correct proxy settings).

7 Click *Finish*, the connection should now succeed.

### Not Enough Space on the Disk

A description of this problem is as follows:

On clicking *OK* in the *Live Update - Select File Groups* dialog, to download the selected files, you get an error message informing you that the disk space required to download all the selected updates exceeds the free disk space.

A suggested solution is to free some disk space on the disk drive where the temporary folder is located until there is enough space to download all the updates. Alternatively, you can de-select updates from the list in the *Live Update - Select File Groups* dialog until the total download size fits into the free disk space.

# A SUPPORTED DEVICES

This appendix details the devices supported by the following features:

- Device View
- Switch Manager
- Device Warranty
- Backup, Restore and Setup
- Agent Update

## Device View

Devices supported by Device View are listed below.

**Table 25** Device View - Supported Devices

| Supported Devices |
|---|
| 3Com AccessBuilder 6218 |
| 3Com AccessBuilder 7000 BRI |
| 3Com AccessBuilder 7000 PRI |
| 3Com CoreBuilder 2500 |
| 3Com CoreBuilder 3500 |
| 3Com CoreBuilder 9000 16-Slot |
| 3Com CoreBuilder 9000 9-Slot |
| 3Com CoreBuilder 9400 |
| 3Com FMS II |
| 3Com LANplex 2016 |
| 3Com LinkSwitch 2200 |
| 3Com OfficeConnect Hub 8TPM |

| Supported Devices |
|---|
| 3Com OfficeConnect Remote 531s |
| 3Com OfficeConnect Switch 140 |
| 3Com SuperStack 3 Switch 3300 |
| 3Com SuperStack ARPS |
| 3Com SuperStack II 3900-24 |
| 3Com SuperStack II 3900-36 |
| 3Com SuperStack II 9300 |
| 3Com SuperStack II Desktop Switch |
| 3Com SuperStack II Dual Speed Hub |
| 3Com SuperStack II Hub 10 |
| 3Com SuperStack II Hub 100 |
| 3Com SuperStack II PS Hub |
| 3Com SuperStack II Switch 1000 |
| 3Com SuperStack II Switch 1100 |
| 3Com SuperStack II Switch 2200 |
| 3Com SuperStack II Switch 2200 |
| 3Com SuperStack II Switch 3000 |
| 3Com SuperStack II Switch 3300 |
| 3Com SuperStack II Switch 3800 |
| 3Com SuperStack II Switch 9000 |
| 3Com SuperStack Switch 9100 |
| 3Com SuperStack 3 Switch 4400 Family |
| 3Com SuperStack 3 Switch 4900 Family |
| 3Com SuperStack II UPS |
| 3Com Switch 4007 |

## Switch Manager

The devices supported by the Switch Manager feature are shown in Table 26:

**Table 26** Switch Manager - Supported Devices

| Supported Devices |
|---|
| 3Com Switch 7700 |

## Router Manager

The devices supported by the Router Manager feature are shown in Table 27:

**Table 27** Router Manager - Supported Devices

| Supported Devices |
|---|
| Router 5009 |
| Router 5231 |
| Router 5640 |
| Router 5680 |
| Router 3012 |
| Router 3013 |
| Router 3016 |

## Device Warranty

The devices supported by the Device Warranty feature are shown in Table 28:

**Table 28** Device Warranty - Supported Devices

| Supported Devices |
|---|
| 3Com CoreBuilder Switch 3500 and modules |
| 3Com LinkBuilder FMS 10BT/FMS 1/FMS II |
| 3Com LinkSwitch 1000 |
| 3Com LinkSwitch 2200 |
| 3Com LinkSwitch 3000 |
| 3Com NetBuilder II, SuperStack II NetBuilder 20x, SuperStack II NetBuilder 42x |

| Supported Devices |
|---|
| 3Com Network Jack 200 |
| 3Com OfficeConnect Hub 8/TPM |
| 3Com OfficeConnect Switch 140M |
| 3Com SuperStack 3 Server Load Balancer family |
| 3Com SuperStack 3 Switch 4200 family |
| 3Com SuperStack 3 Switch 4300 |
| 3Com SuperStack 3 Switch 4400 family |
| 3Com SuperStack 3 Switch 4900 family |
| 3Com SuperStack 3 Webcache 1000 |
| 3Com SuperStack 3 Webcache 3000 |
| 3Com SuperStack II Desktop Switch |
| 3Com SuperStack II Dual Speed Hub 500 |
| 3Com SuperStack II Hub 10/SuperStack II Hub 100 |
| 3Com SuperStack II Layer 3 Switch Module |
| 3Com SuperStack II PS Hub 40/PS Hub 50 |
| 3Com SuperStack II Remote Access System 1500 Base Unit |
| 3Com SuperStack II Switch 1000 |
| 3Com SuperStack II Switch 2200 |
| 3Com SuperStack II Switch 3000 |
| 3Com SuperStack II Switch 3800 |
| 3Com SuperStack II Switch 3900 family |
| 3Com SuperStack II Switch 610 |
| 3Com SuperStack II Switch 630 |
| 3Com SuperStack II Switch 9000 |
| 3Com SuperStack II Switch 9100 |
| 3Com SuperStack II/SuperStack 3 Switch 1100 family |
| 3Com SuperStack II/SuperStack 3 Switch 3300 family |
| 3Com Switch 4005 and modules |

| Supported Devices |
|---|
| 3Com Switch 4007 and modules |
| 3Com Switch 4050 |
| 3Com Switch 4060 |
| 3Com Wireless LAN Access Point 8000/8200 |

## Backup, Restore and Setup

The devices and minimum agent versions supported by Backup, Restore and Setup are shown in Table 29 and are correct at the time of publication.

**Table 29** Supported 3Com Devices and Minimum Agent Versions

| Device Type | Part Number | Minimum Agent Version |
|---|---|---|
| SuperStack II Switch 610 | 3C16954 | 2.6 |
| SuperStack II Switch 630 | 3C16984 | 2.6 |
| SuperStack II Switch 1100 (12 port) | 3C16951 | 2.6 |
| SuperStack II Switch 1100 (24 port) | 3C16950 | 2.6 |
| SuperStack II Switch 3300 (12 port) | 3C16981 | 2.6 |
| SuperStack II Switch 3300 (24 port) | 3C16980 | 2.6 |
| SuperStack II Switch 3300 FX | 3C16982 | 2.6 |
| SuperStack II Switch 3300 XM | 3C16985 | 2.6 |
| SuperStack II Switch 3300 XM | 3C16985A | 2.6 |
| SuperStack II Switch 3300 TM | 3C16986 | 2.6 |
| SuperStack II Switch 3300 SM | 3C16987 | 2.6 |
| SuperStack II Switch 3300 MM | 3C16988 | 2.6 |
| SuperStack 3 Switch 3300 (12 port) | 3C16981A | 2.6 |
| SuperStack 3 Switch 3300 (24 port) | 3C16980A | 2.6 |
| SuperStack 3 Switch 3300 XM | 3C16985B | 2.6 |

| Device Type | Part Number | Minimum Agent Version |
|---|---|---|
| SuperStack 3 Switch 3300 TM | 3C16986A | 2.6 |
| SuperStack 3 Switch 3300 SM | 3C16987A | 2.6 |
| SuperStack 3 Switch 3300 MM | 3C16988A | 2.6 |
| | | |
| SuperStack 3 Switch 4300 | 3C17100 | 1.1 |
| | | |
| SuperStack 3 Switch 4400 (24 port) | 3C17203 | 3.0 |
| SuperStack 3 Switch 4400 (48 port) | 3C17204 | 3.0 |
| SuperStack 3 Switch 4400 SE | 3C17206 | 3.0 |
| | | |
| SuperStack 3 Switch 4900 | 3C17700 | 4.0 |
| SuperStack 3 Switch 4900 SX | 3C17702 | 4.0 |
| SuperStack 3 Switch 4924 | 3C17701 | 4.0 |
| SuperStack 3 Switch 4950 | 3C17706 | 4.0 |
| | | |
| 3Com Switch 4050 | 3C17708 | 4.0 |
| 3Com Switch 4060 | 3C17709 | 4.0 |
| 3Com Switch 4070 | 3C17707 | 4.0 |
| | | |
| Switch 4005: | | |
| Starter Kit/Chassis | 3C1683x / 3C16820 | 2.0 |
| Fabric/Management Module | 3C16824 | 2.0 |
| 1000BASE-SX Module | 3C16825 | 2.0 |
| GBIC Module | 3C16826 | 2.0 |
| 1000BASE-T Module | 3C16827 | 2.0 |
| 10/100BASE-TX Module | 3C16828 | 2.0 |
| 100BASE-FX Module | 3C16829 | 2.0 |

| **Device Type** | **Part Number** | **Minimum Agent Version** |
|---|---|---|
| 1000BASE-T Module 2 port | 3C16841 | 2.0 |
| 1000BASE-SX Module 2 port | 3C16842 | 2.0 |
| GBIC Module 2 port | 3C16843 | 2.0 |
| | | |
| Switch 4007 and 4007R: | | |
| Starter Kit/Chassis (4007) | 3C1681x<br>3C16801 | 3.0.5 |
| Starter Kit/Chassis (4007R) | 3C16804 | 3.0.5 |
| Management Module | 3CB9EME | 3.0.5 |
| 100BASE-FX Switch Module | 3CB9LF20MM | 3.0.5 |
| Fast Ethernet Switch Module | 3CB9LF36R | 3.0.5 |
| Gigabit Ethernet Switch Module | 3CB9LG9MC | 3.0.5 |
| Fast Ethernet Multilayer Switch Module | 3CB9RF12R | 3.0.5 |
| Gigabit Multilayer Switch Module | 3CB9RG4 | 3.0.5 |
| Gigabit Ethernet Switch Fabric (24 port) | 3CB9FG24T | 3.0.5 |
| Gigabit Ethernet Switch Fabric (9 port) | 3CB9FG9 | 3.0.5 |
| Gigabit Ethernet I/O Module | 3CB9LG4 | 3.0.5 |
| Wireless LAN Access Point 8000 | 3CRWE80096A | 1.1 |

*The SuperStack 3 Switch 4400 SE device is supported by Backup, Restore and Setup. However, a License Key is required to enable the Backup and Restore feature in the agent software. Please refer to the user documentation supplied with your switch for details of how to obtain the appropriate License Key.*

## Agent Update

Table 30 shows the devices that are supported by the Agent Update operation.

**Table 30** Supported 3Com Devices and Minimum Agent Versions

| Device Type | Part Number | Minimum Agent Version |
|---|---|---|
| SuperStack II PS Hub 40 (12 Port) | 3C16405 | - |
| SuperStack II PS Hub 40 (24 Port) | 3C16406 | - |
| SuperStack II PS Hub 50 | 3C16450 | - |
| | | |
| SuperStack II DS Hub 500 (12 Port) | 3C16610 | - |
| SuperStack II DS Hub 500 (24 Port) | 3C16611 | - |
| | | |
| SuperStack II Switch 610 | 3C16954 | - |
| SuperStack II Switch 630 | 3C16984 | - |
| SuperStack II Switch 1100 (12 port) | 3C16951 | - |
| SuperStack II Switch 1100 (24 port) | 3C16950 | - |
| | | |
| SuperStack II Switch 3300 (12 port) | 3C16981 | - |
| SuperStack II Switch 3300 (24 port) | 3C16980 | - |
| SuperStack II Switch 3300 XM | 3C16985 | - |
| SuperStack II Switch 3300 XM | 3C16985A | - |
| SuperStack II Switch 3300 SM | 3C16987 | - |
| SuperStack II Switch 3300 TM | 3C16986 | - |
| SuperStack II Switch 3300 MM | 3C16988 | - |
| SuperStack II Switch 3300 FX | 3C16982 | - |
| SuperStack 3 Switch 3300 (12 port) | 3C16981A | - |
| SuperStack 3 Switch 3300 (24 port) | 3C16980A | - |
| SuperStack 3 Switch 3300 MM | 3C16988A | - |

| **Device Type** | **Part Number** | **Minimum Agent Version** |
|---|---|---|
| SuperStack 3 Switch 3300 XM | 3C16985B | - |
| SuperStack 3 Switch 3300 TM | 3C16986A | - |
| SuperStack 3 Switch 3300 SM | 3C16987A | - |
| | | |
| SuperStack 3 Switch 4226T | 3C17300 | - |
| SuperStack 3 Switch 4250T | 3C17302 | - |
| | | |
| SuperStack 3 Switch 4300 | 3C17100 | - |
| | | |
| SuperStack 3 Switch 4400 (24 port) | 3C17203 | - |
| SuperStack 3 Switch 4400 (48 port) | 3C17204 | - |
| SuperStack 3 Switch 4400 SE | 3C17206 | - |
| | | |
| SuperStack 3 Switch 4900 | 3C17700 | - |
| SuperStack 3 Switch 4900 SX | 3C17702 | - |
| SuperStack 3 Switch 4924 | 3C17701 | - |
| SuperStack 3 Switch 4950 | 3C17706 | - |
| | | |
| 3Com Switch 4050 | 3C17708 | - |
| 3Com Switch 4060 | 3C17709 | - |
| 3Com Switch 4070 | 3C17707 | |
| | | |
| Switch 4005: | | |
| Starter Kit/Chassis | 3C1683x<br>3C16820 | 1.2 |
| Fabric/Management Module | 3C16824 | 1.2 |
| 1000BASE-SX Module | 3C16825 | 1.2 |

| Device Type | Part Number | Minimum Agent Version |
|---|---|---|
| GBIC Module | 3C16826 | 1.2 |
| 1000BASE-T Module | 3C16827 | 1.2 |
| 10/100BASE-TX Module | 3C16828 | 1.2 |
| 100BASE-FX Module | 3C16829 | 1.2 |
| 1000BASE-T Module 2 port | 3C16841 | 1.2 |
| 1000BASE-SX Module 2 port | 3C16842 | 1.2 |
| GBIC Module 2 port | 3C16843 | 1.2 |
| | | |
| Wireless LAN Access Point 8000 | 3CRWE80096A | 1.01 |
| | | |
| SuperStack 3 Webcache 1000 | 3C16115 | 2.0 |
| SuperStack 3 Webcache 3000 | 3C16116 | 2.0 |

# B

# 3COM DEVICE VIEW

This appendix describes how 3Com Device View enables you to monitor and set up the 3Com hubs, switches, bridges/routers and remote access devices on your network.

The following is covered in this appendix:

- About Device View
- Management Support Matrix

## About Device View

Device View provides an SNMP-based interface for managing the connectivity devices on your network.

When you manage a device, Device View creates an accurate graphical representation of the hardware that enables you to view the status of ports and indicators. You can use this to set up device and port parameters and collect detailed statistics.

Device View manages 3Com small office, system and multi-function hubs, switches, remote access devices and power systems.

*For a list of supported devices in this release of 3Com Network Administrator refer to Appendix A on page 241.*

## Management Support Matrix

This section details the devices that you can manage with Device View and the management features that are available:

| Monitor status | Setup device | Use SuperStack groups | Upgrade agent software | Manage ports | Manage console port | Manage bridging | Create resilient links | Create VLANs | View statistics | Set up traps | Manage security | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ✓ | ✓ | | | ✓ | | ✓ | | | | ✓ | | 3Com AccessBuilder 6218 |
| ✓ | ✓ | | | ✓ | | ✓ | | | | ✓ | | 3Com AccessBuilder 7000 BRI |
| ✓ | ✓ | | | ✓ | | ✓ | | | | ✓ | | 3Com AccessBuilder 7000 PRI |
| ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | 3Com CoreBuilder 2500 |
| ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | 3Com CoreBuilder 3500 |
| ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | 3Com CoreBuilder 9000 16-Slot |
| ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | 3Com CoreBuilder 9000 8-Slot |
| ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 3Com CoreBuilder 9400 |
| ✓ | ✓ | | ✓ | ✓ | ✓ | | ✓ | | ✓ | ✓ | ✓ | 3Com FMS II |
| ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ | 3Com LANplex 2016 |
| ✓ | ✓ | | | ✓ | ✓ | | ✓ | | ✓ | ✓ | ✓ | 3Com OfficeConnect Hub 8TPM |

| Monitor status | Setup device | Use SuperStack groups | Upgrade agent software | Manage ports | Manage console port | Manage bridging | Create resilient links | Create VLANs | View statistics | Set up traps | Manage security | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ✓ | ✓ | | | ✓ | | ✓ | | | | ✓ | | 3Com OfficeConnect Remote 531 |
| ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | | ✓ | ✓ | ✓ | 3Com OfficeConnect Switch 140 |
| ✓ | ✓ | ✓ | | | | | | | | | | 3Com SuperStack ARPS |
| ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 3Com SuperStack II 3900-24 |
| ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 3Com SuperStack II 9300 |
| ✓ | ✓ | | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 3Com SuperStack II Desktop Switch |
| ✓ | ✓ | | | ✓ | ✓ | | ✓ | | ✓ | ✓ | ✓ | 3Com SuperStack II Dual Speed Hub |
| ✓ | ✓ | | | ✓ | ✓ | | ✓ | | ✓ | ✓ | ✓ | 3Com SuperStack II Hub 10 |
| ✓ | ✓ | | | ✓ | ✓ | | ✓ | | ✓ | ✓ | ✓ | 3Com SuperStack II Hub 100 |
| ✓ | ✓ | | | ✓ | ✓ | | ✓ | | ✓ | ✓ | ✓ | 3Com SuperStack II PS Hub |
| ✓ | ✓ | | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 3Com SuperStack II Switch 1000 |
| ✓ | ✓ | | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 3Com SuperStack II Switch 1100 |
| ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 3Com SuperStack II Switch 2200 |
| ✓ | ✓ | | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 3Com SuperStack II Switch 3000 |
| ✓ | ✓ | | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 3Com SuperStack II Switch 3300 |
| ✓ | ✓ | | | ✓ | | ✓ | | ✓ | ✓ | ✓ | ✓ | 3Com SuperStack II Switch 3800 |
| ✓ | ✓ | | | ✓ | | ✓ | | ✓ | ✓ | ✓ | | 3Com SuperStack II Switch 9000 |
| ✓ | ✓ | | | ✓ | | ✓ | | ✓ | ✓ | ✓ | | 3Com SuperStack II Switch 9100 |
| ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | 3Com Switch 4007 |
| ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 3Com SuperStack 3 Switch 3300 |
| ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 3Com SuperStack 3 Switch 4400-24 |

| Monitor status | Setup device | Use SuperStack groups | Upgrade agent software | Manage ports | Manage console port | Manage bridging | Create resilient links | Create VLANs | View statistics | Set up traps | Manage security | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 3Com SuperStack 3 Switch 4400-48 |
| ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 3Com Superstack 3 Switch 4400 PWR |
| ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 3Com SuperStack 3 Switch 4400 SE |
| ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 3Com SuperStack 3 Switch 4900 |
| ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 3Com SuperStack 3 Switch 4900 SX |
| ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 3Com SuperStack 3 Switch 4924 |
| ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 3Com SuperStack 3 Switch 4950 |

# C OBTAINING SUPPORT FOR YOUR PRODUCT

## Register Your Product to Gain Service Benefits

To take advantage of warranty and other service benefits, you must first register your product at **`http://eSupport.3com.com/`**. 3Com eSupport services are based on accounts that you create or have authorization to access. First time users must apply for a user name and password that provides access to a number of eSupport features including Product Registration, Repair Services, and Service Request.

## Purchase Value-Added Services

To enhance response times or extend warranty benefits, contact 3Com or your authorized 3Com reseller. Value-added services can include 24x7 telephone technical support, software upgrades, onsite assistance or advance hardware replacement. Experienced engineers are available to manage your installation with minimal disruption to your network. Expert assessment and implementation services are offered to fill resource gaps and ensure the success of your networking projects. More information on 3Com Extended Warranty and Professional Services is available at **`http://www.3com.com/`**

Contact your authorized 3Com reseller or 3Com for additional product and support information.

## Troubleshoot Online

You will find support tools posted on the 3Com web site at **`http://www.3com.com/`**

- **3Com Knowledgebase** helps you troubleshoot 3Com products. This query-based interactive tool is located at **`http://knowledgebase.3com.com`** and contains thousands of technical solutions written by 3Com support engineers.
- **Connection Assistant** helps you install, configure and troubleshoot 3Com desktop and server NICs, wireless cards and Bluetooth devices. This diagnostic software is located at:

**http://www.3com.com/prodforms/software/connection_assistant/ca_thankyou.html**

## Access Software Downloads

**Software Updates** are the bug fix / maintenance releases for the version of software initially purchased with the product. In order to access these Software Updates you must first register your product on the 3Com web site at **http://eSupport.3com.com/**.

First time users will need to apply for a user name and password. A link to software downloads can be found at **http://eSupport.3com.com/**, or under the Product Support heading at **http://www.3com.com/**

**Software Upgrades** are the software releases that follow the software version included with your original product. In order to access upgrades and related documentation you must first purchase a service contract from 3Com or your reseller.

## Contact Us

3Com offers telephone, e-mail and internet access to technical support and repair services. To access these services for your region, use the appropriate telephone number, URL or e-mail address from the list below. You will find a current directory of support telephone numbers posted on the 3Com web site at **http://csoweb4.3com.com/contactus/**

## Telephone Technical Support and Repair

To obtain telephone support as part of your warranty and other service benefits, you must first register your product at **http://eSupport.3com.com/**

When you contact 3Com for assistance, please have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision level
- Diagnostic error messages
- Details about recent configuration changes, if applicable

To send a product directly to 3Com for repair, you must first obtain a return authorization number (RMA). Products sent to 3Com, without authorization numbers clearly marked on the outside of the package, will be returned to the sender unopened, at the sender's expense. If your product is registered and under warranty, you can obtain an RMA number online at **`http://eSupport.3com.com/`**. First time users will need to apply for a user name and password.

Telephone numbers are correct at the time of publication. Find a current directory of support telephone numbers posted on the 3Com web site at **`http://csoweb4.3com.com/contactus/`**

| Country | Telephone Number | Country | Telephone Number |
|---|---|---|---|
| **Asia, Pacific Rim Telephone Technical Support and Repair** | | | |
| Australia | 1 800 678 515 | Philippines | 1235 61 266 2602 or<br>1800 1 888 9469 |
| Hong Kong | 800 933 486 | | |
| India | +61 2 9424 5179 or<br>000800 650 1111 | P.R. of China | 10800 61 00137 or<br>021 6350 1590 or<br>00800 0638 3266 |
| Indonesia | 001 803 61009 | | |
| Japan | 00531 616 439 or<br>03 5977 7991 | Singapore | 800 6161 463 |
| | | S. Korea | 080 333 3308 |
| Malaysia | 1800 801 777 | Taiwan | 00801 611 261 |
| New Zealand | 0800 446 398 | Thailand | 001 800 611 2000 |
| Pakistan | +61 2 9937 5083 | | |
| You can also obtain support in this region using the following e-mail: **`apr_technical_support@3com.com`** | | | |
| Or request a repair authorization number (RMA) by fax using this number: | | | + 65 543 6348 |
| **Europe, Middle East, and Africa Telephone Technical Support and Repair** | | | |
| From anywhere in these regions, call: | +44 (0)1442 435529 | | |
| From the following countries, you may use the numbers shown: | | | |
| Austria | 01 7956 7124 | Luxembourg | 342 0808128 |
| Belgium | 070 700 770 | Netherlands | 0900 777 7737 |
| Denmark | 7010 7289 | Norway | 815 33 047 |
| Finland | 01080 2783 | Poland | 00800 441 1357 |
| France | 0825 809 622 | Portugal | 707 200 123 |
| Germany | 01805 404 747 | South Africa | 0800 995 014 |
| Hungary | 06800 12813 | Spain | 9 021 60455 |
| Ireland | 01407 3387 | Sweden | 07711 14453 |
| Israel | 1800 945 3794 | Switzerland | 08488 50112 |
| Italy | 199 161346 | U.K. | 0870 909 3266 |
| You can also obtain support in this region using the following URL: **`http://emea.3com.com/support/email.html`** | | | |

| Country | Telephone Number | Country | Telephone Number |
|---|---|---|---|
| **Latin America Telephone Technical Support and Repair** | | | |
| Antigua | 1 800 988 2112 | Guatemala | AT&T +800 998 2112 |
| Argentina | 0 810 444 3COM | Haiti | 57 1 657 0888 |
| Aruba | 1 800 998 2112 | Honduras | AT&T +800 998 2112 |
| Bahamas | 1 800 998 2112 | Jamaica | 1 800 998 2112 |
| Barbados | 1 800 998 2112 | Martinique | 571 657 0888 |
| Belize | 52 5 201 0010 | Mexico | 01 800 849CARE |
| Bermuda | 1 800 998 2112 | Nicaragua | AT&T +800 998 2112 |
| Bonaire | 1 800 998 2112 | Panama | AT&T +800 998 2112 |
| Brazil | 0800 13 3COM | Paraguay | 54 11 4894 1888 |
| Cayman | 1 800 998 2112 | Peru | AT&T +800 998 2112 |
| Chile | AT&T +800 998 2112 | Puerto Rico | 1 800 998 2112 |
| Colombia | AT&T +800 998 2112 | Salvador | AT&T +800 998 2112 |
| Costa Rica | AT&T +800 998 2112 | Trinidad and Tobago | 1 800 998 2112 |
| Curacao | 1 800 998 2112 | Uruguay | AT&T +800 998 2112 |
| Ecuador | AT&T +800 998 2112 | Venezuela | AT&T +800 998 2112 |
| Dominican Republic | AT&T +800 998 2112 | Virgin Islands | 57 1 657 0888 |

You can also obtain support in this region using the following:

Spanish speakers, enter the URL:
**`http://lat.3com.com/lat/support/form.html`**

Portuguese speakers, enter the URL:
**`http://lat.3com.com/br/support/form.html`**

English speakers in Latin America should send e-mail to:
**`lat_support_anc@3com.com`**

| | | | |
|---|---|---|---|
| **US and Canada Telephone Technical Support and Repair** | | | |
| | 1 800 876 3266 | | |

# D SYSTEM REQUIREMENTS

This appendix details the system requirements needed in order to utilize 3Com Network Administrator.

## Operating System

There are two supported platforms for 3Com Network Administrator which are:

- Windows 2000 Professional SP2
- Windows XP Professional SP1

## Web Browser

3Com Network Administrator supports the following web browsers:

- Netscape Navigator 4.x and above
- Netscape 7
- Internet Explorer 4.x and above

*There is no support for any version of Netscape 6.*

## HP OpenView Supported Versions

3Com Network Administrator supports HP OpenView versions 6.2, 6.4 and 7.0.

## Additional Software Required

Adobe Acrobat Reader is required to view the PDF files installed with 3Com Network Administrator. This is included on the CD.

## Hardware

The minimum hardware specification required for 3Com Network Administrator is:

- IBM PC or compatible, with 266 MHz Pentium II processor
- 256MB RAM
- 250MB free hard disk space
- 1024 x 768 graphics capabilities with 256 colors
- CD-ROM drive
- Network adapter card

The recommended hardware specifications for 3Com Network Administrator is:

- IBM PC or compatible, with 1 GHz Pentium III processor, or above
- 512MB RAM or more
- 250MB free hard disk space
- 1024 x 768 graphics capabilities with 64K colors
- CD-ROM drive
- Network adapter card

*The hardware specifications are the 3Com Network Administrator minimum and recommended specifications. These do not represent the hardware specifications for HP OpenView.*

# INDEX

# 3COM End User Software License Agreement

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE USING THIS PRODUCT. IT CONTAINS SOFTWARE, THE USE OF WHICH IS LICENSED BY 3COM CORPORATION ("3COM") TO ITS CUSTOMERS FOR THEIR USE ONLY AS SET FORTH BELOW. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT USE OR INSTALL THE SOFTWARE. USING OR INSTALLING ANY PART OF THE SOFTWARE INDICATES THAT YOU ACCEPT THESE TERMS.

## LICENSE

3Com grants you a nonexclusive license to use the accompanying software program(s) (the "Software") subject to the terms and restrictions set forth in this License Agreement. You are not permitted to lease, rent, distribute or sublicense the Software or to use the Software in a time-sharing arrangement or in any other unauthorized manner. Further, no license is granted to you in the human readable code of the Software (source code). Except as provided below, this License Agreement does not grant you any rights to patents, copyrights trade secrets, trademarks, or any other rights in respect to the Software.

The Software is licensed to be used on any workstation (provided that the Software is used only in connection with a 3Com internetworking product) or on any 3Com internetworking product, owned by or leased to you. You may reproduce and provide one (1) copy of the Software and supporting documentation for each such workstation or 3Com internetworking product on which the Software is used as permitted hereunder. Otherwise, the Software and supporting documentation may be copied only as essential for backup or archive purposes in support of your use of the Software as permitted hereunder. You must reproduce and include all copyright notices and any other proprietary rights notices appearing on the Software and the supporting documentation on any copies that you make.

## NO ASSIGNMENT; NO REVERSE ENGINEERING

You may not transfer or assign the Software and/or this License Agreement to another party without the prior written consent of 3Com. If such consent is given and you transfer or assign the Software and/or this License Agreement, then you must at the same time either transfer any copies of the Software as well as the supporting documentation to the same party or destroy any such materials not transferred. Except as set forth above, you may not transfer or assign the Software or your rights under this License Agreement.

Modification, reverse engineering, reverse compiling, or disassembly of the Software is expressly prohibited. However, if you are a European Community ("EC") resident, information necessary to achieve interoperability of the Software with other programs within the meaning of the EC Directive on the Legal Protection of Computer Programs is available to you from 3Com upon written request.

## EXPORT RESTRICTIONS

You agree that you will not export or re-export the Software or accompanying documentation (or any copies thereof) or any products utilizing the Software or such documentation in violation of any applicable laws or regulations of the United States and the country in which you obtained them.

## TRADE SECRETS; TITLE

You acknowledge and agree that the structure, sequence and organization of the Software are the valuable trade secrets of 3Com and its suppliers. You agree to hold such trade secrets in confidence. You further acknowledge and agree that ownership of, and title to, the Software and all subsequent copies thereof regardless of the form or media are held by 3Com and its suppliers.

## UNITED STATES GOVERNMENT LEGEND

The Software is commercial in nature and developed solely at private expense. The Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a commercial item as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in this License Agreement, which is 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov. 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided in any licensed program or documentation to you under this License Agreement.

## TERM AND TERMINATION

This license will expire fifty (50) years from the date that you open the package, if it is not earlier terminated. You may terminate it at any time by destroying the Software and documentation together with all copies and merged portions in any form. It will also terminate immediately if you fail to comply with any term or condition of this License Agreement. Upon such termination you agree to destroy the Software and documentation, together with all copies and merged portions in any form.

## GOVERNING LAW

This License Agreement shall be governed by the laws of England. You agree that the United Nations Convention on Contracts for the International Sale of Goods (1980) is hereby excluded in its entirety from application to this License Agreement.

## NO WARRANTY

THE SOFTWARE AND RELATED DOCUMENTATION ARE PROVIDED ON AN "AS IS" BASIS AND ALL RISK IS WITH YOU. 3COM MAKES NO WARRANTIES OR CONDITIONS, EXPRESS, IMPLIED OR STATUTORY AS TO ANY MATTER WHATSOEVER REGARDING THE SOFTWARE AND DOCUMENTATION. IN PARTICULAR, ANY AND ALL WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTIES RIGHTS ARE EXPRESSLY EXCLUDED. FURTHER, 3COM MAKES NO REPRESENTATIONS, WARRANTIES OR CONDITIONS THAT THE SOFTWARE AND DOCUMENTATION PROVIDED ARE FREE OF ERRORS OR VIRUSES, OR THAT THE SOFTWARE AND DOCUMENTATION ARE SUITABLE FOR YOUR INTENDED USE.

## LIMITATION OF LIABILITY

IN NO EVENT SHALL 3COM OR ITS SUPPLIERS BE LIABLE TO YOU OR ANY OTHER PARTY FOR ANY INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, LOSS OF DATA OR DATA BEING RENDERED INACCURATE, LOSS OF PROFITS OR REVENUE, OR INTERRUPTION OF BUSINESS IN ANY WAY ARISING OUT OF OR RELATED TO THE USE OR INABILITY TO USE THE SOFTWARE AND/OR DOCUMENTATION, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT PRODUCT LIABILITY OR OTHERWISE, EVEN IF ANY REPRESENTATIVE OF 3COM OR ITS SUPPLIERS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. NOTHING IN THIS AGREEMENT SHALL HAVE THE EFFECT OF LIMITING OR EXCLUDING 3COM'S LIABILITY FOR DEATH OR PERSONAL INJURY CAUSED BY ITS OWN NEGLIGENCE.

## DISCLAIMER

Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to you. This warranty gives you specific legal rights which may vary depending on local law.

## SEVERABILITY

In the event any provision of this License Agreement is found to be invalid, illegal or unenforceable, the validity, legality and enforceability of any of the remaining provisions shall not in any way be affected or impaired and a valid, legal and enforceable provision of similar intent and economic impact shall be substituted therefor.

## ENTIRE AGREEMENT

This License Agreement sets forth the entire understanding and agreement between you and 3Com, supersedes all prior agreements, whether written or oral, with respect to the Software, and may be amended only in a writing signed by both parties.

3Com is a registered trademark of 3Com Corporation.

3Com Corporation, 350 Campus Drive

Marlborough

MA USA 01752-3064